

ATTACHED APPENDICES

Appendix A	Standard Clauses for New York State Contracts
Appendix B	General Specifications
Appendix C	Equal Employment Opportunity Staffing Plan
Appendix D	Glossary of Terms
Appendix E	Volumes
Appendix F	NYS GIS Program Office Geocoding Services
Appendix G	Sample Forms
Appendix H	FBI CJS Cards
Appendix I	NYS DMV Requirements
Appendix J	Standardized Reports
Appendix K	Information Sharing Environment, Functional Standard Suspicious Activity Reporting
Appendix L	Data Structure SJS
Appendix M	Data Structure ACISS
Appendix N	Proposed Staffing and Title Threshold
Appendix O	List of Law Enforcement Agencies
Appendix P	Contract Modification Procedures
Appendix Q	CJS Security Policy v5

APPENDIX A

STANDARD CLAUSES FOR NEW YORK STATE CONTRACTS

**PLEASE RETAIN THIS DOCUMENT
FOR FUTURE REFERENCE.**

TABLE OF CONTENTS

	Page
1. Executory Clause	3
2. Non-Assignment Clause	3
3. Comptroller's Approval	3
4. Workers' Compensation Benefits	3
5. Non-Discrimination Requirements	3
6. Wage and Hours Provisions	3
7. Non-Collusive Bidding Certification	4
8. International Boycott Prohibition	4
9. Set-Off Rights	4
10. Records	4
11. Identifying Information and Privacy Notification	4
12. Equal Employment Opportunities For Minorities and Women	4-5
13. Conflicting Terms	5
14. Governing Law	5
15. Late Payment	5
16. No Arbitration	5
17. Service of Process	5
18. Prohibition on Purchase of Tropical Hardwoods	5-6
19. MacBride Fair Employment Principles	6
20. Omnibus Procurement Act of 1992	6
21. Reciprocity and Sanctions Provisions	6
22. Compliance with New York State Information Security Breach and Notification Act	6
23. Compliance with Consultant Disclosure Law	6
24. Procurement Lobbying	7
25. Certification of Registration to Collect Sales and Compensating Use Tax by Certain State Contractors, Affiliates and Subcontractors	7
26. Iran Divestment Act	7

STANDARD CLAUSES FOR NYS CONTRACTS

The parties to the attached contract, license, lease, amendment or other agreement of any kind (hereinafter, "the contract" or "this contract") agree to be bound by the following clauses which are hereby made a part of the contract (the word "Contractor" herein refers to any party other than the State, whether a contractor, licenser, licensee, lessor, lessee or any other party):

1. EXECUTORY CLAUSE. In accordance with Section 41 of the State Finance Law, the State shall have no liability under this contract to the Contractor or to anyone else beyond funds appropriated and available for this contract.

2. NON-ASSIGNMENT CLAUSE. In accordance with Section 138 of the State Finance Law, this contract may not be assigned by the Contractor or its right, title or interest therein assigned, transferred, conveyed, sublet or otherwise disposed of without the State's previous written consent, and attempts to do so are null and void. Notwithstanding the foregoing, such prior written consent of an assignment of a contract let pursuant to Article XI of the State Finance Law may be waived at the discretion of the contracting agency and with the concurrence of the State Comptroller where the original contract was subject to the State Comptroller's approval, where the assignment is due to a reorganization, merger or consolidation of the Contractor's business entity or enterprise. The State retains its right to approve an assignment and to require that any Contractor demonstrate its responsibility to do business with the State. The Contractor may, however, assign its right to receive payments without the State's prior written consent unless this contract concerns Certificates of Participation pursuant to Article 5-A of the State Finance Law.

3. COMPTROLLER'S APPROVAL. In accordance with Section 112 of the State Finance Law (or, if this contract is with the State University or City University of New York, Section 355 or Section 6218 of the Education Law), if this contract exceeds \$50,000 (or the minimum thresholds agreed to by the Office of the State Comptroller for certain S.U.N.Y. and C.U.N.Y. contracts), or if this is an amendment for any amount to a contract which, as so amended, exceeds said statutory amount, or if, by this contract, the State agrees to give something other than money when the value or reasonably estimated value of such consideration exceeds \$10,000, it shall not be valid, effective or binding upon the State until it has been approved by the State Comptroller and filed in his office. Comptroller's approval of contracts let by the Office of General Services is required when such contracts exceed \$85,000 (State Finance Law Section 163.6-a). However, such pre-approval shall not be required for any contract established as a centralized contract through the Office of General Services or for a purchase order or other transaction issued under such centralized contract.

4. WORKERS' COMPENSATION BENEFITS. In accordance with Section 142 of the State Finance Law, this

contract shall be void and of no force and effect unless the Contractor shall provide and maintain coverage during the life of this contract for the benefit of such employees as are required to be covered by the provisions of the Workers' Compensation Law.

5. NON-DISCRIMINATION REQUIREMENTS. To the extent required by Article 15 of the Executive Law (also known as the Human Rights Law) and all other State and Federal statutory and constitutional non-discrimination provisions, the Contractor will not discriminate against any employee or applicant for employment because of race, creed, color, sex (including gender identity or expression), national origin, sexual orientation, military status, age, disability, predisposing genetic characteristics, marital status or domestic violence victim status. Furthermore, in accordance with Section 220-e of the Labor Law, if this is a contract for the construction, alteration or repair of any public building or public work or for the manufacture, sale or distribution of materials, equipment or supplies, and to the extent that this contract shall be performed within the State of New York, Contractor agrees that neither it nor its subcontractors shall, by reason of race, creed, color, disability, sex, or national origin: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. If this is a building service contract as defined in Section 230 of the Labor Law, then, in accordance with Section 239 thereof, Contractor agrees that neither it nor its subcontractors shall by reason of race, creed, color, national origin, age, sex or disability: (a) discriminate in hiring against any New York State citizen who is qualified and available to perform the work; or (b) discriminate against or intimidate any employee hired for the performance of work under this contract. Contractor is subject to fines of \$50.00 per person per day for any violation of Section 220-e or Section 239 as well as possible termination of this contract and forfeiture of all moneys due hereunder for a second or subsequent violation.

6. WAGE AND HOURS PROVISIONS. If this is a public work contract covered by Article 8 of the Labor Law or a building service contract covered by Article 9 thereof, neither Contractor's employees nor the employees of its subcontractors may be required or permitted to work more than the number of hours or days stated in said statutes, except as otherwise provided in the Labor Law and as set forth in prevailing wage and supplement schedules issued by the State Labor Department. Furthermore, Contractor and its subcontractors must pay at least the prevailing wage rate and pay or provide the prevailing supplements, including the premium rates for overtime pay, as determined by the State Labor Department in accordance with the Labor Law. Additionally, effective April 28, 2008, if this is a public work contract covered by Article 8 of the Labor Law, the Contractor understands and agrees that the filing of payrolls in a manner consistent with Subdivision 3-a of Section 220 of the Labor Law shall be a condition precedent to payment by the State of

any State approved sums due and owing for work done upon the project.

7. NON-COLLUSIVE BIDDING CERTIFICATION. In accordance with Section 139-d of the State Finance Law, if this contract was awarded based upon the submission of bids, Contractor affirms, under penalty of perjury, that its bid was arrived at independently and without collusion aimed at restricting competition. Contractor further affirms that, at the time Contractor submitted its bid, an authorized and responsible person executed and delivered to the State a non-collusive bidding certification on Contractor's behalf.

8. INTERNATIONAL BOYCOTT PROHIBITION. In accordance with Section 220-f of the Labor Law and Section 139-h of the State Finance Law, if this contract exceeds \$5,000, the Contractor agrees, as a material condition of the contract, that neither the Contractor nor any substantially owned or affiliated person, firm, partnership or corporation has participated, is participating, or shall participate in an international boycott in violation of the federal Export Administration Act of 1979 (50 USC App. Sections 2401 et seq.) or regulations thereunder. If such Contractor, or any of the aforesaid affiliates of Contractor, is convicted or is otherwise found to have violated said laws or regulations upon the final determination of the United States Commerce Department or any other appropriate agency of the United States subsequent to the contract's execution, such contract, amendment or modification thereto shall be rendered forfeit and void. The Contractor shall so notify the State Comptroller within five (5) business days of such conviction, determination or disposition of appeal (2NYCRR 105.4).

9. SET-OFF RIGHTS. The State shall have all of its common law, equitable and statutory rights of set-off. These rights shall include, but not be limited to, the State's option to withhold for the purposes of set-off any moneys due to the Contractor under this contract up to any amounts due and owing to the State with regard to this contract, any other contract with any State department or agency, including any contract for a term commencing prior to the term of this contract, plus any amounts due and owing to the State for any other reason including, without limitation, tax delinquencies, fee delinquencies or monetary penalties relative thereto. The State shall exercise its set-off rights in accordance with normal State practices including, in cases of set-off pursuant to an audit, the finalization of such audit by the State agency, its representatives, or the State Comptroller.

10. RECORDS. The Contractor shall establish and maintain complete and accurate books, records, documents, accounts and other evidence directly pertinent to performance under this contract (hereinafter, collectively, "the Records"). The Records must be kept for the balance of the calendar year in which they were made and for six (6) additional years thereafter. The State Comptroller, the Attorney General and any other person or entity authorized to conduct an examination, as well as the agency or agencies involved in this

contract, shall have access to the Records during normal business hours at an office of the Contractor within the State of New York or, if no such office is available, at a mutually agreeable and reasonable venue within the State, for the term specified above for the purposes of inspection, auditing and copying. The State shall take reasonable steps to protect from public disclosure any of the Records which are exempt from disclosure under Section 87 of the Public Officers Law (the "Statute") provided that: (i) the Contractor shall timely inform an appropriate State official, in writing, that said records should not be disclosed; and (ii) said records shall be sufficiently identified; and (iii) designation of said records as exempt under the Statute is reasonable. Nothing contained herein shall diminish, or in any way adversely affect, the State's right to discovery in any pending or future litigation.

11. IDENTIFYING INFORMATION AND PRIVACY NOTIFICATION.

(a) Identification Number(s). Every invoice or New York State Claim for Payment submitted to a New York State agency by a payee, for payment for the sale of goods or services or for transactions (e.g., leases, easements, licenses, etc.) related to real or personal property must include the payee's identification number. The number is any or all of the following: (i) the payee's Federal employer identification number, (ii) the payee's Federal social security number, and/or (iii) the payee's Vendor Identification Number assigned by the Statewide Financial System. Failure to include such number or numbers may delay payment. Where the payee does not have such number or numbers, the payee, on its invoice or Claim for Payment, must give the reason or reasons why the payee does not have such number or numbers.

(b) Privacy Notification. (1) The authority to request the above personal information from a seller of goods or services or a lessor of real or personal property, and the authority to maintain such information, is found in Section 5 of the State Tax Law. Disclosure of this information by the seller or lessor to the State is mandatory. The principal purpose for which the information is collected is to enable the State to identify individuals, businesses and others who have been delinquent in filing tax returns or may have understated their tax liabilities and to generally identify persons affected by the taxes administered by the Commissioner of Taxation and Finance. The information will be used for tax administration purposes and for any other purpose authorized by law. (2) The personal information is requested by the purchasing unit of the agency contracting to purchase the goods or services or lease the real or personal property covered by this contract or lease. The information is maintained in the Statewide Financial System by the Vendor Management Unit within the Bureau of State Expenditures, Office of the State Comptroller, 110 State Street, Albany, New York 12236.

12. EQUAL EMPLOYMENT OPPORTUNITIES FOR MINORITIES AND WOMEN.

In accordance with Section 312 of the Executive Law and 5 NYCRR 143, if this contract is: (i) a written agreement or purchase order instrument, providing for a total expenditure in excess of \$25,000.00,

whereby a contracting agency is committed to expend or does expend funds in return for labor, services, supplies, equipment, materials or any combination of the foregoing, to be performed for, or rendered or furnished to the contracting agency; or (ii) a written agreement in excess of \$100,000.00 whereby a contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon; or (iii) a written agreement in excess of \$100,000.00 whereby the owner of a State assisted housing project is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon for such project, then the following shall apply and by signing this agreement the Contractor certifies and affirms that it is Contractor's equal employment opportunity policy that:

(a) The Contractor will not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability or marital status, shall make and document its conscientious and active efforts to employ and utilize minority group members and women in its work force on State contracts and will undertake or continue existing programs of affirmative action to ensure that minority group members and women are afforded equal employment opportunities without discrimination. Affirmative action shall mean recruitment, employment, job assignment, promotion, upgradings, demotion, transfer, layoff, or termination and rates of pay or other forms of compensation;

(b) at the request of the contracting agency, the Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, labor union or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability or marital status and that such union or representative will affirmatively cooperate in the implementation of the Contractor's obligations herein; and

(c) the Contractor shall state, in all solicitations or advertisements for employees, that, in the performance of the State contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

Contractor will include the provisions of "a", "b", and "c" above, in every subcontract over \$25,000.00 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor. Section 312 does not apply to: (i) work, goods or services unrelated to this contract; or (ii) employment outside New York State. The State shall consider compliance by a contractor or subcontractor with the requirements of any federal law concerning equal employment

opportunity which effectuates the purpose of this section. The contracting agency shall determine whether the imposition of the requirements of the provisions hereof duplicate or conflict with any such federal law and if such duplication or conflict exists, the contracting agency shall waive the applicability of Section 312 to the extent of such duplication or conflict. Contractor will comply with all duly promulgated and lawful rules and regulations of the Department of Economic Development's Division of Minority and Women's Business Development pertaining hereto.

13. CONFLICTING TERMS. In the event of a conflict between the terms of the contract (including any and all attachments thereto and amendments thereof) and the terms of this Appendix A, the terms of this Appendix A shall control.

14. GOVERNING LAW. This contract shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise.

15. LATE PAYMENT. Timeliness of payment and any interest to be paid to Contractor for late payment shall be governed by Article 11-A of the State Finance Law to the extent required by law.

16. NO ARBITRATION. Disputes involving this contract, including the breach or alleged breach thereof, may not be submitted to binding arbitration (except where statutorily authorized), but must, instead, be heard in a court of competent jurisdiction of the State of New York.

17. SERVICE OF PROCESS. In addition to the methods of service allowed by the State Civil Practice Law & Rules ("CPLR"), Contractor hereby consents to service of process upon it by registered or certified mail, return receipt requested. Service hereunder shall be complete upon Contractor's actual receipt of process or upon the State's receipt of the return thereof by the United States Postal Service as refused or undeliverable. Contractor must promptly notify the State, in writing, of each and every change of address to which service of process can be made. Service by the State to the last known address shall be sufficient. Contractor will have thirty (30) calendar days after service hereunder is complete in which to respond.

18. PROHIBITION ON PURCHASE OF TROPICAL HARDWOODS. The Contractor certifies and warrants that all wood products to be used under this contract award will be in accordance with, but not limited to, the specifications and provisions of Section 165 of the State Finance Law, (Use of Tropical Hardwoods) which prohibits purchase and use of tropical hardwoods, unless specifically exempted, by the State or any governmental agency or political subdivision or public benefit corporation. Qualification for an exemption under this law will be the responsibility of the contractor to establish to meet with the approval of the State.

In addition, when any portion of this contract involving the use of woods, whether supply or installation, is to be performed by any subcontractor, the prime Contractor will indicate and certify in the submitted bid proposal that the subcontractor has been informed and is in compliance with specifications and provisions regarding use of tropical hardwoods as detailed in §165 State Finance Law. Any such use must meet with the approval of the State; otherwise, the bid may not be considered responsive. Under bidder certifications, proof of qualification for exemption will be the responsibility of the Contractor to meet with the approval of the State.

19. MACBRIDE FAIR EMPLOYMENT PRINCIPLES.

In accordance with the MacBride Fair Employment Principles (Chapter 807 of the Laws of 1992), the Contractor hereby stipulates that the Contractor either (a) has no business operations in Northern Ireland, or (b) shall take lawful steps in good faith to conduct any business operations in Northern Ireland in accordance with the MacBride Fair Employment Principles (as described in Section 165 of the New York State Finance Law), and shall permit independent monitoring of compliance with such principles.

20. OMNIBUS PROCUREMENT ACT OF 1992. It is the policy of New York State to maximize opportunities for the participation of New York State business enterprises, including minority and women-owned business enterprises as bidders, subcontractors and suppliers on its procurement contracts.

Information on the availability of New York State subcontractors and suppliers is available from:

NYS Department of Economic Development
Division for Small Business
Albany, New York 12245
Telephone: 518-292-5100
Fax: 518-292-5884
email: opa@esd.ny.gov

A directory of certified minority and women-owned business enterprises is available from:

NYS Department of Economic Development
Division of Minority and Women's Business Development
633 Third Avenue
New York, NY 10017
212-803-2414
email: mwbecertification@esd.ny.gov
<https://ny.newnycontracts.com/FrontEnd/VendorSearchPublic.asp>

The Omnibus Procurement Act of 1992 requires that by signing this bid proposal or contract, as applicable, Contractors certify that whenever the total bid amount is greater than \$1 million:

(a) The Contractor has made reasonable efforts to encourage the participation of New York State Business Enterprises as suppliers and subcontractors, including certified minority and women-owned business enterprises, on this project, and has retained the documentation of these efforts to be provided upon request to the State;

(b) The Contractor has complied with the Federal Equal Opportunity Act of 1972 (P.L. 92-261), as amended;

(c) The Contractor agrees to make reasonable efforts to provide notification to New York State residents of employment opportunities on this project through listing any such positions with the Job Service Division of the New York State Department of Labor, or providing such notification in such manner as is consistent with existing collective bargaining contracts or agreements. The Contractor agrees to document these efforts and to provide said documentation to the State upon request; and

(d) The Contractor acknowledges notice that the State may seek to obtain offset credits from foreign countries as a result of this contract and agrees to cooperate with the State in these efforts.

21. RECIPROCITY AND SANCTIONS PROVISIONS.

Bidders are hereby notified that if their principal place of business is located in a country, nation, province, state or political subdivision that penalizes New York State vendors, and if the goods or services they offer will be substantially produced or performed outside New York State, the Omnibus Procurement Act 1994 and 2000 amendments (Chapter 684 and Chapter 383, respectively) require that they be denied contracts which they would otherwise obtain. NOTE: As of May 15, 2002, the list of discriminatory jurisdictions subject to this provision includes the states of South Carolina, Alaska, West Virginia, Wyoming, Louisiana and Hawaii. Contact NYS Department of Economic Development for a current list of jurisdictions subject to this provision.

22. COMPLIANCE WITH NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT.

Contractor shall comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law Section 899-aa; State Technology Law Section 208).

23. COMPLIANCE WITH CONSULTANT DISCLOSURE LAW.

If this is a contract for consulting services, defined for purposes of this requirement to include analysis, evaluation, research, training, data processing, computer programming, engineering, environmental, health, and mental health services, accounting, auditing, paralegal, legal or similar services, then, in accordance with Section 163 (4-g) of the State Finance Law (as amended by Chapter 10 of the Laws of 2006), the Contractor shall timely, accurately and properly comply with the requirement to submit an annual employment report for the contract to the agency that awarded

the contract, the Department of Civil Service and the State Comptroller.

24. PROCUREMENT LOBBYING. To the extent this agreement is a "procurement contract" as defined by State Finance Law Sections 139-j and 139-k, by signing this agreement the contractor certifies and affirms that all disclosures made in accordance with State Finance Law Sections 139-j and 139-k are complete, true and accurate. In the event such certification is found to be intentionally false or intentionally incomplete, the State may terminate the agreement by providing written notification to the Contractor in accordance with the terms of the agreement.

25. CERTIFICATION OF REGISTRATION TO COLLECT SALES AND COMPENSATING USE TAX BY CERTAIN STATE CONTRACTORS, AFFILIATES AND SUBCONTRACTORS.

To the extent this agreement is a contract as defined by Tax Law Section 5-a, if the contractor fails to make the certification required by Tax Law Section 5-a or if during the term of the contract, the Department of Taxation and Finance or the covered agency, as defined by Tax Law 5-a, discovers that the certification, made under penalty of perjury, is false, then such failure to file or false certification shall be a material breach of this contract and this contract may be terminated, by providing written notification to the Contractor in accordance with the terms of the agreement, if the covered agency determines that such action is in the best interest of the State.

26. IRAN DIVESTMENT ACT. By entering into this Agreement, Contractor certifies in accordance with State Finance Law §165-a that it is not on the "Entities Determined to be Non-Responsive Bidders/Offerers pursuant to the New York State Iran Divestment Act of 2012" ("Prohibited Entities List") posted at:
<http://www.ogs.ny.gov/about/regs/docs/ListofEntities.pdf>

Contractor further certifies that it will not utilize on this Contract any subcontractor that is identified on the Prohibited Entities List. Contractor agrees that should it seek to renew or extend this Contract, it must provide the same certification at the time the Contract is renewed or extended. Contractor also agrees that any proposed Assignee of this Contract will be required to certify that it is not on the Prohibited Entities List before the contract assignment will be approved by the State.

During the term of the Contract, should the state agency receive information that a person (as defined in State Finance Law §165-a) is in violation of the above-referenced certifications, the state agency will review such information and offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment activity which is in violation of the Act within 90 days after the determination of such violation, then the state agency shall take such action as may be appropriate and provided for by law, rule, or contract, including, but not

limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Contractor in default.

The state agency reserves the right to reject any bid, request for assignment, renewal or extension for an entity that appears on the Prohibited Entities List prior to the award, assignment, renewal or extension of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the Prohibited Entities list after contract award.

APPENDIX B
GENERAL SPECIFICATIONS

PLEASE RETAIN THIS DOCUMENT FOR FUTURE REFERENCE

GENERAL

1. APPLICABILITY The terms and conditions set forth in this Appendix B are expressly incorporated in and applicable to the resulting procurement contracts let by the Office of General Services Procurement Services Group, or let by any other Authorized User where incorporated by reference in its Bid Documents. Captions are intended as descriptive and are not intended to limit or otherwise restrict the terms and conditions set forth herein.

2. GOVERNING LAW This procurement, the resulting contract and any purchase orders issued hereunder shall be governed by the laws of the State of New York except where the Federal supremacy clause requires otherwise, and actions or proceedings arising from the contract shall be heard in a court of competent jurisdiction in the State of New York.

3. ETHICS COMPLIANCE All Bidders/Contractors and their employees must comply with the requirements of Sections 73 and 74 of the Public Officers Law, other State codes, rules, regulations and executive orders establishing ethical standards for the conduct of business with New York State. In signing the Bid, Bidder certifies full compliance with those provisions for any present or future dealings, transactions, sales, contracts, services, offers, relationships, etc., involving New York State and/or its employees. Failure to comply with those provisions may result in disqualification from the Bidding process, termination of contract, and/or other civil or criminal proceedings as required by law.

4. (RESERVED)

5. DEFINITIONS Terms used in this Appendix B shall have the following meanings:

AFFILIATE Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) that effectively controls another company in which (a) the Bidder owns more than 50% of the ownership; or (b) any individual or other legal entity which owns more than 50% of the ownership of the Bidder. In addition, if a Bidder owns less than 50% of the ownership of another legal entity, but directs or has the right to direct such entity's daily operations, that entity will be an Affiliate.

AGENCY OR AGENCIES The State of New York, acting by or through one or more departments, boards, commissions, offices or institutions of the State of New York.

ATTORNEY GENERAL Attorney General of the State of New York.

BID OR BID PROPOSAL An offer or proposal submitted by a Bidder to furnish a described product or a solution, perform services or means of achieving a practical end, at a stated price for the stated Contract term. As required by the Bid Documents, the Bid or proposal may be subject to modification through the solicitation by the Agency of best and final offers during the evaluation process prior to recommendation for award of the Contract.

BIDDER/OFFERER Any individual or other legal entity (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) which submits a Bid in response to a Bid Solicitation. The term Bidder shall also include the term "offeror." In the case of negotiated Contracts, "Bidder" shall refer to the "Contractor."

BID DOCUMENTS Writings by the State setting forth the scope, terms, conditions and technical specifications for a procurement of Product. Such writings typically include, but are not limited to: Invitation for Bids (IFB), Request for Quotation (RFQ), Request for Proposals (RFP), addenda or amendments thereto, and terms and conditions which are incorporated by reference, including but not limited to, Appendix A (Standard Clauses for NYS Contracts), and Appendix B, (General Specifications). Where these General Specifications are incorporated in negotiated Contracts that have not been competitively Bid, the term "Bid Documents" shall be deemed to refer to the terms and conditions set forth in the negotiated Contract and associated documentation.

BID SPECIFICATION A written description drafted by the Authorized User setting forth the specific terms of the intended procurement, which may include: physical or functional characteristics, the nature of a commodity or construction item, any description of the work to be performed, Products to be provided, the necessary qualifications of the Bidder, the capacity and capability of the Bidder to successfully carry out the proposed Contract, or the process for achieving specific results and/or anticipated outcomes or any other requirement necessary to perform work. Where these General Specifications are incorporated in negotiated Contracts that have not been competitively Bid, the term "Bid Specifications" shall be deemed to refer to the terms and conditions set forth in the negotiated Contract and associated documentation.

COMMISSIONER Commissioner of OGS, or in the case of Bid Specifications issued by an Authorized User, the head of such Authorized User or their authorized representative.

COMPTROLLER Comptroller of the State of New York.

CONTRACT The writing(s) which contain the agreement of the Commissioner and the Bidder/Contractor setting forth the total legal obligation between the parties as determined by applicable rules of law, and which most typically include the following classifications of public procurements:

a. Agency Specific Contracts Contracts where the specifications for a Product or a particular scope of work are described and defined to meet the needs of one or more Authorized User(s).

b. Centralized Contracts Single or multiple award Contracts where the specifications for a Product or general scope of work are described and defined by the Office of General Services to meet the needs of Authorized Users. Centralized Contracts may be awarded through multiple awards or through adoption of another jurisdiction's contract or on a sole source, single source, emergency or competitive basis. Once established, procurements may be made from the selected Contractor(s) without further competition or Mini-Bid unless otherwise required by the Bid Specifications or Contract Award Notification.

c. Back-Drop Contracts Multiple award Centralized Contracts where the Office of General Services defines the specifications for a Product or general scope of work to meet the needs of Authorized Users. Bids may be submitted either at a date and time certain or may be accepted on a continuous or periodic recruitment basis, as set forth in the Bid Specifications. Selection of a Contractor(s) from among Back-Drop contract holders for an actual Product, project or particular scope of work may subsequently be made on a single or sole source basis, or on the basis of a Mini-Bid among qualified Back-Drop contract holders, or such other method as set forth in the Bid Document.

d. Piggyback Contract A Contract let by any department, agency or instrumentality of the United States government, or any department, agency, office, political subdivision or instrumentality of any state or state(s) which is adopted and extended for use by the OGS Commissioner in accordance with the requirements of the State Finance Law.

e. Contract Letter A letter to the successful Bidder(s) indicating acceptance of its Bid in response to a solicitation. Unless otherwise specified, the issuance of a Letter of Acceptance forms a Contract but is not an order for Product, and Contractor should not take any action with respect to actual Contract deliveries except on the basis of Purchase Orders sent from Authorized User(s).

CONTRACT AWARD NOTIFICATION An announcement to Authorized Users that a Contract has been established.

CONTRACTOR Any successful Bidder(s) to whom a Contract has been awarded by the Commissioner.

DOCUMENTATION The complete set of manuals (e.g., user, installation, instruction or diagnostic manuals) in either hard or electronic copy, which are necessary to enable an Authorized User to properly test, install, operate and enjoy full use of the Product.

EMERGENCY An urgent and unexpected requirement where health and public safety or the conservation of public resources is at risk.

ENTERPRISE The total business operations in the United States of Authorized User (s) without regard to geographic location where such operations are performed or the entity actually performing such operations on behalf of Authorized User.

ENTERPRISE LICENSE A license grant of unlimited rights to deploy, access, use and execute Product anywhere within the Enterprise up to the maximum capacity stated on the Purchase Order or in the Contract.

ERROR CORRECTIONS Machine executable software code furnished by Contractor which corrects the Product so as to conform to the applicable warranties, performance standards and/or obligations of the Contractor.

GROUP A classification of Product, services or technology which is designated by OGS.

INVITATION FOR BIDS (IFB) A type of Bid Document which is most typically used where requirements can be stated and award will be made based on lowest price to the responsive and responsible Bidder(s).

LICENSED SOFTWARE Software transferred upon the terms and conditions set forth in the Contract. "Licensed Software" includes error corrections, upgrades, enhancements or new releases, and any deliverables due under a maintenance or service contract (e.g., patches, fixes, PTFs, programs, code or data conversion, or custom programming).

LICENSEE One or more Authorized Users who acquire Product from Contractor by issuing a Purchase Order in accordance with the terms and conditions of the Contract; provided that, for purposes of compliance with an individual license, the term "Licensee" shall be deemed to refer separately to the individual Authorized User(s) who took receipt of and who is executing the Product, and who shall be solely responsible for performance and liabilities incurred. In the case

of acquisitions by State Agencies, the Licensee shall be the State of New York.

LICENSE EFFECTIVE DATE The date Product is delivered to an Authorized User. Where a License involves Licensee's right to copy a previously licensed and delivered Master Copy of a Program, the license effective date for additional copies shall be deemed to be the date on which the Purchase Order is executed.

LICENSOR A Contractor who transfers rights in proprietary Product to Authorized Users in accordance with the rights and obligations specified in the Contract.

MINI-BID PROJECT DEFINITION A Bid Document containing project specific Bid Specifications developed by or for an Authorized User which solicits Bids from Contractors previously qualified under a Back-Drop Contract.

MULTIPLE AWARD A determination and award of a Contract in the discretion of the Commissioner to more than one responsive and responsible Bidder who meets the requirements of a specification, where the multiple award is made on the grounds set forth in the Bid Document in order to satisfy multiple factors and needs of Authorized Users (e.g., complexity of items, various manufacturers, differences in performance required to accomplish or produce required end results, production and distribution facilities, price, compliance with delivery requirements, geographic location or other pertinent factors).

NEW PRODUCT RELEASES (Product Revisions) Any commercially released revisions to the licensed version of a Product as may be generally offered and available to Authorized Users. New releases involve a substantial revision of functionality from a previously released version of the Product.

OGS The New York State Office of General Services.

PROCUREMENT RECORD Documentation by the Authorized User of the decisions made and approach taken during the procurement process and during the contract term.

PRODUCT A deliverable under any Bid or Contract which may include commodities, services and/or technology. The term "Product" includes Licensed Software.

PROPRIETARY Protected by secrecy, patent, copyright or trademark against commercial competition.

PURCHASE ORDER The Authorized User's fiscal form or format that is used when making a purchase (e.g., formal written Purchase Order, Procurement Card, electronic Purchase Order, or other authorized instrument).

REQUEST FOR PROPOSALS (RFP) A type of Bid Document that is used for procurements where factors in addition to cost are considered and weighted in awarding the contract and where the method of award is "best value," as defined by the State Finance Law.

REQUEST FOR QUOTATION (RFQ) A type of Bid Document that can be used when a formal Bid opening is not required (e.g., discretionary, sole source, single source or emergency purchases).

RESPONSIBLE BIDDER A Bidder that is determined to have financial and organizational capacity, legal authority, satisfactory previous performance, skill, judgment and integrity, and that is found to be competent, reliable and experienced, as determined by the Commissioner. For purposes of being deemed responsible, a Bidder

must also be determined to be in compliance with Sections 139-j and 139-k of the State Finance Law relative to restrictions on contacts during the procurement process and disclosure of contacts and prior findings of non-responsibility under these statutes.

RESPONSIVE BIDDER A Bidder meeting the specifications or requirements prescribed in the Bid Document or solicitation, as determined by the OGS Commissioner.

SINGLE SOURCE A procurement where two or more Bidders can supply the required Product, and the Commissioner may award the contract to one Bidder over the other.

SITE The location (street address) where Product will be executed or services delivered.

SOLE SOURCE A procurement where only one Bidder is capable of supplying the required Product.

SOURCE CODE The programming statements or instructions written and expressed in any language understandable by a human being skilled in the art which are translated by a language compiler to produce executable machine Object Code.

STATE State of New York.

SUBCONTRACTOR Any individual or other legal entity, (including but not limited to sole proprietor, partnership, limited liability company, firm or corporation) who has entered into a contract, express or implied, for the performance of a portion of a Contract with a Contractor.

TERMS OF LICENSE The terms and conditions set forth in the Contract that are in effect and applicable to a Purchase Order at the time of order placement.

VIRUS Any computer code, whether or not written or conceived by Contractor, that disrupts, disables, harms, or otherwise impedes in any manner the operation of the Product, or any other associated software, firmware, hardware, or computer system (such as local area or wide-area networks), including aesthetic disruptions or distortions, but does not include security keys or other such devices installed by Product manufacturer.

BID SUBMISSION

6. INTERNATIONAL BIDDING All offers (tenders), and all information and Product required by the solicitation or provided as explanation thereof, shall be submitted in English. All prices shall be expressed, and all payments shall be made, in United States Dollars (\$US). Any offers (tenders) submitted which do not meet the above criteria will be rejected.

7. BID OPENING Bids may, as applicable, be opened publicly. The Commissioner reserves the right at any time to postpone or cancel a scheduled Bid opening.

8. BID SUBMISSION All Bids are to be packaged, sealed and submitted to the location stated in the Bid Specifications. Bidders are solely responsible for timely delivery of their Bids to the location set forth in the Bid Specifications prior to the stated Bid opening date/time.

A Bid return envelope, if provided with the Bid Specifications, should be used with the Bid sealed inside. If the Bid response does not fit into

the envelope, the Bid envelope should be attached to the outside of the sealed box or package with the Bid inside. If using a commercial delivery company that requires use of their shipping package or envelope, Bidder's sealed Bid, labeled as detailed below, should be placed within the shipper's sealed envelope to ensure that the Bid is not prematurely opened.

All Bids must have a label on the outside of the package or shipping container outlining the following information:

"BID ENCLOSED (bold print, all capitals)

- Group Number
- IFB or RFP Number
- Bid Submission date and time"

In the event that a Bidder fails to provide such information on the return Bid envelope or shipping material, the receiving entity reserves the right to open the shipping package or envelope to determine the proper Bid number or Product group, and the date and time of Bid opening. Bidder shall have no claim against the receiving entity arising from such opening and such opening shall not affect the validity of the Bid or the procurement.

Notwithstanding the receiving agency's right to open a Bid to ascertain the foregoing information, Bidder assumes all risk of late delivery associated with the Bid not being identified, packaged or labeled in accordance with the foregoing requirements.

All Bids must be signed by a person authorized to commit the Bidder to the terms of the Bid Documents and the content of the Bid (offer).

9. (RESERVED)

10. (RESERVED)

11. (RESERVED)

12. BID CONTENTS Bids must be complete and legible. All Bids must be signed. All information required by the Bid Specifications must be supplied by the Bidder on the forms or in the format specified. No alteration, erasure or addition is to be made to the Bid Documents. Changes may be ignored by the Commissioner or may be grounds for rejection of the Bid. Changes, corrections and/or use of white-out in the Bid or Bidder's response portion of the Bid Document must be initialed by an authorized representative of the Bidder. Bidders are cautioned to verify their Bids before submission, as amendments to Bids or requests for withdrawal of Bids received by the Commissioner after the time specified for the Bid opening, may not be considered.

13. EXTRANEIOUS TERMS Bids must conform to the terms set forth in the Bid Documents, as extraneous terms or material deviations (including additional, inconsistent, conflicting or alternative terms) may render the Bid non-responsive and may result in rejection of the Bid.

Extraneous term(s) submitted on standard, pre-printed forms (including but not limited to: product literature, order forms, license agreements, contracts or other documents) that are attached or referenced with submissions shall not be considered part of the Bid or resulting Contract, but shall be deemed included for informational or promotional purposes only.

Only those extraneous terms that meet all the following requirements may be considered as having been submitted as part of the Bid:

- a. Each proposed extraneous term (addition, deletion, counter-offer, deviation, or modification) must be specifically enumerated in a writing which is not part of a pre-printed form; and
- b. The writing must identify the particular specification requirement (if any) that Bidder rejects or proposes to modify by inclusion of the extraneous term; and
- c. The Bidder shall enumerate the proposed addition, counter offer, modification or deviation from the Bid Document, and the reasons therefore.

No extraneous term(s), whether or not deemed "material," shall be incorporated into a Contract or Purchase Order unless submitted in accordance with the above and the Commissioner or Authorized User expressly accepts each such term(s) in writing. Acceptance and/or processing of the Bid shall not constitute such written acceptance of Extraneous Term(s).

14. CONFIDENTIAL/TRADE SECRET MATERIALS

a. **Contractor** Confidential, trade secret or proprietary materials as defined by the laws of the State of New York must be clearly marked and identified as such upon submission by the Bidder. Marking the Bid as "confidential" or "proprietary" on its face or in the document header or footer shall not be considered by the Commissioner or Authorized User to be sufficient without specific justification as to why disclosure of particular information in the Bid would cause substantial injury to the competitive position of the Bidder. Bidders/Contractors intending to seek an exemption from disclosure of these materials under the Freedom of Information Law must request the exemption in writing, setting forth the reasons for the claimed exemption. Acceptance of the claimed materials does not constitute a determination on the exemption request, which determination will be made in accordance with statutory procedures. Properly identified information that has been designated confidential, trade secret, or proprietary by the Bidder will not be disclosed except as may be required by the Freedom of Information Law or other applicable State and federal laws.

b. **Commissioner or Authorized User** Contractor further warrants, covenants and represents that any confidential information obtained by Contractor, its agents, Subcontractors, officers, distributors, resellers or employees in the course of performing its obligations, including without limitation, security procedures, business operations information, or commercial proprietary information in the possession of the State or any Authorized User hereunder or received from another third party, will not be divulged to any third parties. Contractor shall not be required to keep confidential any such material that is publicly available through no fault of Contractor, independently developed by Contractor without reliance on confidential information of the Authorized User, or otherwise obtained under the Freedom of Information Act or other applicable New York State laws and regulations. This warranty shall survive termination of this Contract. Contractor further agrees to take appropriate steps as to its agents, Subcontractors, officers, distributors, resellers or employees regarding the obligations arising under this clause to insure such confidentiality.

15. RELEASE OF BID EVALUATION MATERIALS Requests concerning the evaluation of Bids may be submitted under the Freedom of Information Law. Information, other than statistical or factual tabulations or data such as the Bid Tabulation, shall only be released as required by law after Contract award. Bid Tabulations are not maintained for all procurements. Names of Bidders may be disclosed after Bid opening upon request. Written requests should be directed to the Commissioner.

16. FREEDOM OF INFORMATION LAW During the evaluation process, the content of each Bid will be held in confidence and details of any Bid will not be revealed (except as may be required under the Freedom of Information Law or other State law). The Freedom of Information Law provides for an exemption from disclosure for trade secrets or information the disclosure of which would cause injury to the competitive position of commercial enterprises. This exception would be effective both during and after the evaluation process. If the Bid contains any such trade secret or other confidential or proprietary information, it must be accompanied in the Bid with a written request to the Commissioner to not disclose such information. Such request must state with particularity the reasons why the information should not be available for disclosure and must be provided at the time of submission of the Bid. Notations in the header, footer or watermark of the Bid Document will not be considered sufficient to constitute a request for non-disclosure of trade secret or other confidential or proprietary information. Where a Freedom of Information request is made for trademark or other confidential or proprietary information, the Commissioner reserves the right to determine upon written notice to the Bidder whether such information qualifies for the exemption for disclosure under the law. Notwithstanding the above, where a Bid tabulation is prepared and Bids publicly opened, such Bid tabulation shall be available upon request.

17. PREVAILING WAGE RATES - PUBLIC WORKS AND BUILDING SERVICES CONTRACTS If any portion of work being Bid is subject to the prevailing wage rate provisions of the Labor Law, the following shall apply:

a. **"Public Works" and "Building Services" - Definitions**

i. **Public Works** Labor Law Article 8 applies to contracts for public improvement in which laborers, workers or mechanics are employed on a "public works" project (distinguished from public "procurement" or "service" contracts). The State, a public benefit corporation, a municipal corporation (including a school district), or a commission appointed by law must be a party to the Contract. The wage and hours provision applies to any work performed by Contractor or Subcontractors.

ii. **Building Services** Labor Law Article 9 applies to Contracts for building service work over \$1,500 with a public agency, that: (i) involve the care or maintenance of an existing building, or (ii) involve the transportation of office furniture or equipment to or from such building, or (iii) involve the transportation and delivery of fossil fuel to such building, and (iv) the principal purpose of which is to furnish services through use of building service employees.

b. **Prevailing Wage Rate Applicable to Bid Submissions** A copy of the applicable prevailing wage rates to be paid or provided are annexed to the Bid Documents. Bidders must submit Bids which are based upon the prevailing hourly wages, and supplements in cash or equivalent benefits (i.e., fringe benefits and any cash or non-cash compensation which are not wages, as defined by law) that equal or exceed the applicable prevailing wage rate(s) for the location where the work is to be performed. Bidders may not submit Bids based upon hourly wage rates and supplements below the applicable prevailing wage rates as established by the New York State Department of Labor. **Bids that fail to comply with this requirement will be disqualified.**

c. **Wage Rate Payments / Changes During Contract Term** The wages to be paid under any resulting Contract shall not be less than the prevailing rate of wages and supplements as set forth by law. It is required that the Contractor keep informed of all changes in the Prevailing Wage Rates during the Contract term that apply to the classes of individuals supplied by the Contractor on any projects resulting from this Contract, subject to the provisions of the Labor

Law. Contractor is solely liable for and must pay such required prevailing wage adjustments during the Contract term as required by law.

d. Public Posting & Certified Payroll Records In compliance with Article 8, Section 220 of the New York State Labor Law:

i. Posting The Contractor must publicly post on the work site, in a prominent and accessible place, a legible schedule of the prevailing wage rates and supplements.

ii. Payroll Records Contractors and Subcontractors must keep original payrolls or transcripts subscribed and affirmed as true under the penalties of perjury as required by law. For public works contracts over \$25,000 where the Contractor maintains no regular place of business in New York State, such records must be kept at the work site. For building services contracts, such records must be kept at the work site while work is being performed.

iii. Submission of Certified Payroll Transcripts for Public Works Contracts Only Contractors and Subcontractors on public works projects must submit monthly payroll transcripts to the Authorized User that has prepared or directs the preparation of the plans and specifications for a public works project, as set forth in the Bid Specifications. For Mini-Bid solicitations, the payroll records must be submitted to the entity preparing the agency Mini-Bid project specification. For "agency specific" Bids, the payroll records should be submitted to the entity issuing the purchase order. For all other OGS Centralized Contracts, such records should be submitted to the individual agency issuing the purchase order(s) for the work. Upon mutual agreement of the Contractor and the Authorized User, the form of submission may be submitted in a specified disk format acceptable to the Department of Labor provided: 1) the Contractor/Subcontractor retains the original records; and, (2) an original signed letter by a duly authorized individual of the Contractor or Subcontractor attesting to the truth and accuracy of the records accompanies the disk. This provision does not apply to Article 9 of the Labor Law building services contracts.

iv. Records Retention Contractors and Subcontractors must preserve such certified transcripts for a period of three years from the date of completion of work on the awarded contract.

Day's Labor Eight hours shall constitute a legal day's work for all classes of employees in this state except those engaged in farm and domestic service unless otherwise provided by law.

No laborers, workmen or mechanics in the employ of the Contractor, Subcontractor or other person doing or contracting to do all or part of the work contemplated by the Contract shall be permitted or required to work more than eight hours in any one calendar day or more than five calendar days in any one week except in cases of extraordinary emergency including fire, flood or danger to life or property. "Extraordinary emergency" shall be deemed to include situations in which sufficient laborers, workers and mechanics cannot be employed to carry on public work expeditiously as a result of such restrictions upon the number of hours and days of labor and the immediate commencement or prosecution or completion without undue delay of the public work is necessary in the judgment of the NYS Commissioner of Labor for the preservation of the Contract site or for the protection of the life and limb of the persons using the Contract site.

18. TAXES

a. Unless otherwise specified in the Bid Specifications or Contract, the quoted Bid price includes all taxes applicable to the transaction.

b. Purchases made by the State of New York and certain non-State Authorized Users are exempt from New York State and local sales taxes and, with certain exceptions, federal excise taxes. To satisfy the requirements of the New York State Sales tax exemption, either the Purchase Order issued by a State Agency or the invoice forwarded to authorize payment for such purchases will be sufficient evidence that the sale by the Contractor was made to the State, an exempt organization under Section 1116 (a) (1) of the Tax Law. Non-State Authorized Users must offer their own proof of exemption upon request. No person, firm or corporation is, however, exempt from paying the State Truck Mileage and Unemployment Insurance or Federal Social Security taxes, which remain the sole responsibility of the Bidder/Contractor.

c. Pursuant to Revised Tax Law 5-a, Contractor will be required to furnish sales tax certification on its behalf and for its affiliates, and subcontractors for Contracts with a value greater than \$100,000 in accordance with provisions of the law.

d. Purchases by Authorized Users other than the State of New York may be subject to certain taxes which were not included in the Bid price, and in those instances the tax should be computed based on the Contract price and added to the invoice submitted to such entity for payment.

19. EXPENSES PRIOR TO CONTRACT EXECUTION The Commissioner and any Authorized User(s) are not liable for any costs incurred by a Vendor, Bidder or Contractor in the preparation and production of a Bid, Mini-Bid or best and final offers or for any work performed prior to Contract execution.

20. ADVERTISING RESULTS The prior written approval of the Commissioner is required in order for results of the Bid to be used by the Contractor as part of any commercial advertising. The Contractor shall also obtain the prior written approval of the Commissioner relative to the Bid or Contract for press or other media releases.

21. (RESERVED)

22. REMANUFACTURED, RECYCLED, RECYCLABLE OR RECOVERED MATERIALS Upon the conditions specified in the Bid Specifications and in accordance with the laws of the State of New York, Contractors are encouraged to use recycled, recyclable or recovered materials in the manufacture of Products and packaging to the maximum extent practicable without jeopardizing the performance or intended end use of the Product or packaging unless such use is precluded due to health, welfare, safety requirements or in the Bid Specifications. Contractors are further encouraged to offer remanufactured Products to the maximum extent practicable without jeopardizing the performance or intended end use of the Product and unless such use is precluded due to health, welfare, safety requirements or by the Bid Specifications. Where such use is not practical, suitable, or permitted by the Bid Specifications, Contractor shall deliver new materials in accordance with the "Warranties" set forth below.

Items with recycled, recyclable, recovered, refurbished or remanufactured content must be identified in the Bid or Bidder will be deemed to be offering new Product.

23. (RESERVED)

24. PRICING

a. **Unit Pricing** If required by the Bid Specifications, the Bidder should insert the price per unit specified and the price extensions in

decimals, not to exceed four places for each item unless otherwise specified, in the Bid. In the event of a discrepancy between the unit price and the extension, the unit price shall govern unless, in the sole judgment of the Commissioner, such unit pricing is obviously erroneous.

b. Net Pricing Unless otherwise required by the Bid Specifications, prices shall be net, including transportation, customs, tariff, delivery and other charges fully prepaid by the Contractor to the destination(s) indicated in the Bid Specifications, subject to the cash discount.

c. “No Charge” Bid When Bids are requested on a number of Products as a Group or Lot, a Bidder desiring to Bid “no charge” on a Product in the Group or Lot must clearly indicate such. Otherwise, such Bid may be considered incomplete and be rejected, in whole or in part, at the discretion of the Commissioner.

d. Educational Pricing All Products to be supplied for educational purposes that are subject to educational discounts shall be identified in the Bid and such discounts shall be made available to qualifying institutions.

e. Third Party Financing If Product acquisitions are financed through any third party financing, Contractor may be required as a condition of Contract Award to agree to the terms and conditions of a “Consent & Acknowledgment Agreement” in a form acceptable to the Commissioner.

f. Best Pricing Offer During the Contract term, if substantially the same or a smaller quantity of a Product is sold by the Contractor outside of this Contract upon the same or similar terms and conditions as that of this Contract at a lower price to a federal, state or local governmental entity, the price under this Contract, at the discretion of the Commissioner, shall be immediately reduced to the lower price.

Price decreases shall take effect automatically during the Contract term and apply to Purchase Orders submitted on or after:

(i) GSA Changes: Where NYS Net Prices are based on an approved GSA Schedule, the date the approved GSA Schedule pricing decreases during the Contract term; or

(ii) Commercial Price List Reductions: Where NYS Net Prices are based on a discount from Contractor’s list prices, the date Contractor lowers its pricing to its customers generally or to similarly situated government customers during the Contract term; or

(iii) Special Offers/Promotions Generally: Where Contractor generally offers more advantageous special price promotions or special discount pricing to other customers during the Contract term for a similar quantity, and the maximum price or discount associated with such offer or promotion is better than the discount or Net Price otherwise available under this Contract, such better price or discount shall apply for similar quantity transactions under this Contract for the life of such general offer or promotion; and

(iv) Special Offers/Promotions to Authorized Users: Contractor may offer Authorized Users, under either this Contract or any other Contracting vehicle, competitive pricing which is lower than the NYS Net Price set forth herein at any time during the Contract term and such lower pricing shall not be applied as a global price reduction under the Contract pursuant to the foregoing paragraph (iii).

Unless otherwise specified in the Bid Specifications, Contractor may offer lower prices or better terms (see Modification of Contract Terms) on any specific Purchase Order(s) from any Authorized User without being in conflict with, or obligation to comply on a global basis, with the terms of this clause.

g. Best and Final Prices As specified in the Bid Documents and Contract, a Contractor may be solicited at the time of issuance of a Purchase Order or Mini-Bid award for best and final pricing for the Product or service to be delivered to the Authorized User. Contractors are encouraged to reduce their pricing upon receipt of such request.

25. DRAWINGS

a. Drawings Submitted With Bid When the Bid Specifications require the Bidder to furnish drawings and/or plans, such drawings and/or plans shall conform to the mandates of the Bid Documents and shall, when approved by the Commissioner, be considered a part of the Bid and of any resulting Contract. All symbols and other representations appearing on the drawings shall be considered a part of the drawing.

b. Drawings Submitted During the Contract Term Where required to develop, maintain and deliver diagrams or other technical schematics regarding the scope of work, Contractor shall do so on an ongoing basis at no additional charge, and must, as a condition of payment, update drawings and plans during the Contract term to reflect additions, alterations, and deletions. Such drawings and diagrams shall be delivered to the Authorized User’s representative.

c. Accuracy of Drawings Submitted All drawings shall be neat and professional in manner and shall be clearly labeled as to locations and type of product, connections and components. Drawings and diagrams are to be in compliance with accepted drafting standards. Acceptance or approval of such plans shall not relieve the Contractor from responsibility for design or other errors of any sort in the drawings or plans, or from its responsibility for performing as required, furnishing product, services or installation, or carrying out any other requirements of the intended scope of work.

26. (RESERVED)

27. PROCUREMENT CARD The State has entered into an agreement for purchasing card services. The Purchasing Card enables Authorized Users to make authorized purchases directly from a Contractor without processing a Purchase Orders or Purchase Authorizations. Purchasing Cards are issued to selected employees authorized to purchase for the Authorized User and having direct contact with Contractors. Cardholders can make purchases directly from any Contractor that accepts the Purchasing Card.

The Contractor shall not process a transaction for payment through the credit card clearinghouse until the purchased products have been shipped or services performed. Unless the cardholder requests correction or replacement of a defective or faulty Product in accordance with other Contract requirements, the Contractor shall immediately credit a cardholder’s account for products returned as defective or faulty.

28. (RESERVED)

BID EVALUATION

29. BID EVALUATION The Commissioner reserves the right to accept or reject any and all Bids, or separable portions of offers, and waive technicalities, irregularities, and omissions if the Commissioner determines the best interests of the State will be served. The Commissioner, in his/her sole discretion, may accept or reject illegible, incomplete or vague Bids and his/her decision shall be final. A conditional or revocable Bid which clearly communicates the terms or limitations of acceptance may be considered, and Contract award may be made in compliance with the Bidder’s conditional or revocable terms in the offer.

30. (RESERVED)

31. CLARIFICATIONS / REVISIONS Prior to award, the Commissioner reserves the right to seek clarifications, request Bid revisions, or to request any information deemed necessary for proper evaluation of Bids from all Bidders deemed to be eligible for Contract award. Failure to provide requested information may result in rejection of the Bid.

32. PROMPT PAYMENT DISCOUNTS While prompt payment discounts will not be considered in determining the low Bid, the Commissioner may consider any prompt payment discount in resolving Bids which are otherwise tied. However, any notation indicating that the price is net, (e.g., net 30 days), shall be understood to mean only that no prompt payment discount is offered by the Bidder. The imposition of service, interest, or other charges, except pursuant to the provisions of Article 11-A of the State Finance Law, which are applicable in any case, may render the Bid non-responsive and may be cause for its rejection.

33. (RESERVED)

34. PERFORMANCE AND RESPONSIBILITY QUALIFICATIONS The Commissioner reserves the right to investigate or inspect at any time whether or not the Product, services, qualifications or facilities offered by the Bidder/Contractor meet the requirements set forth in the Bid Specifications/Contract or as set forth during Contract negotiations. Contractor shall at all times during the Contract term remain responsible and responsive. A Bidder/Contractor must be prepared, if requested by the Commissioner, to present evidence of legal authority to do business in New York State, integrity, experience, ability, prior performance, organizational and financial capacity as well as where applicable, a statement as to supply, plant, machinery and capacity of the manufacturer or source for the production, distribution and servicing of the Product offered/Bid. If the Commissioner determines that the conditions and terms of the Bid Documents, Bid Specifications or Contract are not complied with, or that items, services or Product proposed to be furnished do not meet the specified requirements, or that the legal authority, integrity experience, ability, prior performance, organization and financial capacity or facilities are not satisfactory, the Commissioner may reject such Bid or terminate the Contract.

35. DISQUALIFICATION FOR PAST PERFORMANCE AND FINDINGS OF NON-RESPONSIBILITY Bidder may be disqualified from receiving awards if Bidder, or anyone in Bidder's employment, has previously failed to perform satisfactorily in connection with public Bidding or contracts or is deemed non-responsible.

36. QUANTITY CHANGES PRIOR TO AWARD The Commissioner reserves the right, at any time prior to the award of a specific quantity Contract, to alter in good faith the quantities listed in the Bid Specifications. In the event such right is exercised, the lowest responsible Bidder meeting Bid Specifications will be advised of the revised quantities and afforded an opportunity to extend or reduce its Bid price in relation to the changed quantities. Refusal by the low Bidder to so extend or reduce its Bid price may result in the rejection of its Bid and the award of such Contract to the lowest responsible Bidder who accepts the revised qualifications.

37. (RESERVED)**TERMS & CONDITIONS**

38. CONTRACT CREATION / EXECUTION Except for contracts governed by Article 11-B of the State Finance Law, subject to and upon receipt of all required approvals as set forth in the Bid Specifications a Contract shall be deemed executed and created with the successful Bidder(s), upon the Commissioner's mailing or electronic communication to the address on the Bid/Contract of: (i) the final Contract Award Notice; (ii) a fully executed Contract; or (iii) a Purchase Order authorized by the Commissioner.

39. PARTICIPATION IN CENTRALIZED CONTRACTS The following shall not limit or inhibit the OGS Commissioner's authority under State Finance Law, Section 163 (10) (e) (Piggybacking):

a. (RESERVED)

b. (RESERVED)

c. (RESERVED)

d. **Responsibility for Performance** Participation in state Centralized Contracts by Authorized Users is permitted upon the following conditions: (i) the responsibility with regard to performance of any contractual obligation, covenant, condition or term thereunder by any Authorized User other than State Agencies shall be borne and is expressly assumed by such Authorized User and not by the State; (ii) a breach of the Contract by any particular Authorized User shall neither constitute nor be deemed a breach of the Contract as a whole which shall remain in full force and effect, and shall not affect the validity of the Contract nor the obligations of the Contractor thereunder respecting non-breaching Authorized Users, whether State or otherwise; (iii) for a breach by an Authorized User other than a State Agency, the State specifically and expressly disclaims any and all liability for such breach; and (iv) each non-state agency Authorized User and Contractor guarantees to save the State, its officers, agents and employees harmless from any liability that may be or is imposed by their failure to perform in accordance with its obligations under the Contract.

e. **Contract Migration** Authorized Users holding individual Contracts with a Contractor at the time that Contractor is awarded a Centralized Contract for the same Products or services shall be permitted to migrate to that Centralized Contract effective with its commencement date. Such migration shall not operate to diminish, alter or eliminate any right that the Authorized User otherwise had under the terms and conditions of their individual Contract.

40. MODIFICATION OF CONTRACT TERMS The terms and conditions set forth in the Contract shall govern all transactions by Authorized User(s) under this Contract. The Contract may only be modified or amended upon mutual written agreement of the Commissioner and Contractor.

The Contractor may, however, offer Authorized User(s) more advantageous pricing, payment, or other terms and conditions than those set forth in the Contract. In such event, a copy of such terms shall be furnished to the Authorized User(s) and Commissioner by the Contractor at the time of such offer.

Other than where such terms are more advantageous for the Authorized User(s) than those set forth in the Contract, no alteration or modification of the terms of the Contract, including substitution of Product, shall be valid or binding against Authorized User(s) unless authorized by the Commissioner or specified in the Contract Award

Notification. No such alteration or modification shall be made by unilaterally affixing such terms to Product upon delivery (including, but not limited to, attachment or inclusion of standard pre-printed order forms, product literature, "shrink wrap" terms accompanying software upon delivery, or other documents) or by incorporating such terms onto order forms, purchase orders or other documents forwarded by the Contractor for payment, notwithstanding Authorized User's subsequent acceptance of Product, or that Authorized User has subsequently processed such document for approval or payment.

41. SCOPE CHANGES The Commissioner reserves the right, unilaterally, to require, by written order, changes by altering, adding to or deducting from the Bid Specifications, such changes to be within the general scope of the Contract. The Commissioner may make an equitable adjustment in the Contract price or delivery date if the change affects the cost or time of performance. Such equitable adjustments require the consent of the Contractor, which consent shall not be unreasonably withheld.

42. (RESERVED)

43. EMERGENCY CONTRACTS In the event that a disaster emergency is declared by Executive Order under Section 28 of Article 2-B of the Executive Law, or the Commissioner determines pursuant to his/her authority under Section 163 (10) (b) of the State Finance Law that an emergency exists requiring the prompt and immediate delivery of Product, the Commissioner reserves the right to obtain such Product from any source, including but not limited to this Contract(s), as the Commissioner in his/her sole discretion determines will meet the needs of such emergency. Contractor shall not be entitled to any claim or lost profits for Product procured from other sources pursuant to this paragraph. The reasons underlying the finding that an emergency exists shall be included in the procurement record.

44. PURCHASE ORDERS Unless otherwise authorized in writing by the Commissioner, no Product is to be delivered or furnished by Contractor until transmittal of an official Purchase Order from the Authorized User. Unless terminated or cancelled pursuant to the authority vested in the Commissioner, Purchase Orders shall be effective and binding upon the Contractor when placed in the mail or electronically transmitted prior to the termination of the contract period, addressed to the Contractor at the address for receipt of orders set forth in the Contract or in the Contract Award Notification.

All Purchase Orders issued pursuant to Contracts let by the Commissioner must bear the appropriate Contract number and, if necessary, required State approvals. As deemed necessary, the Authorized User may confirm pricing and other Product information with the Contractor prior to placement of the Purchase Order. The State reserves the right to require any other information from the Contractor which the State deems necessary in order to complete any Purchase Order placed under the Contract. Unless otherwise specified, all Purchase Orders against Centralized Contracts will be placed by Authorized Users directly with the Contractor and any discrepancy between the terms stated on the vendor's order form, confirmation or acknowledgment, and the Contract terms shall be resolved in favor of the terms most favorable to the Authorized User. Should an Authorized User add written terms and conditions to the Purchase Order that conflict with the terms and conditions of the Contract, the Contractor has the option of rejecting the Purchase Order within five business days of its receipt but shall first attempt to negotiate the additional written terms and conditions in good faith with the Authorized User, or fulfill the Purchase Order. Notwithstanding the above, the Authorized User reserves the right to dispute any discrepancies arising from the presentation of additional terms and conditions with the Contractor.

If, with respect to an Agency Specific Contract let by the OGS Commissioner, a Purchase Order is not received by the Contractor within two weeks after the issuance of a Contract Award Notification, it is the responsibility of the Contractor to request in writing that the appropriate Authorized User forward a Purchase Order. If, thereafter, a Purchase Order is not received within a reasonable period of time, the Contractor shall promptly notify in writing the appropriate purchasing officer in OGS. Failure to timely notify such officer may, in the discretion of the OGS Commissioner and without cost to the State, result in the cancellation of such requirement by the OGS Commissioner with a corresponding reduction in the Contract quantity and price.

45. (RESERVED)

46. (RESERVED)

47. (RESERVED)

48. TITLE AND RISK OF LOSS Notwithstanding the form of shipment, title or other property interest, risk of loss shall not pass from the Contractor to the Authorized User until the Products have been received, inspected and accepted by the receiving entity. Acceptance shall occur within a reasonable time or in accordance with such other defined acceptance period as may be specified in the Bid Specifications or Purchase Order. Mere acknowledgment by Authorized User personnel of the delivery or receipt of goods (e.g., signed bill of lading) shall not be deemed or construed as acceptance of the Products received. Any delivery of Product that is substandard or does not comply with the Bid Specifications or Contract terms and conditions, may be rejected or accepted on an adjusted price basis, as determined by the Commissioner.

49. (RESERVED)

50. (RESERVED)

51. (RESERVED)

52. INSTALLATION Where installation is required, Contractor shall be responsible for placing and installing the Product in the required locations. All materials used in the installation shall be of good quality and shall be free from any and all defects that would mar the appearance of the Product or render it structurally unsound. Installation includes the furnishing of any equipment, rigging and materials required to install or place the Product in the proper location. The Contractor shall protect the site from damage for all its work and shall repair damages or injury of any kind caused by the Contractor, its employees, officers or agents. If any alteration, dismantling or excavation, etc. is required to effect installation, the Contractor shall thereafter promptly restore the structure or site. Work shall be performed to cause the least inconvenience to the Authorized User(s) and with proper consideration for the rights of other Contractors or workers. The Contractor shall promptly perform its work and shall coordinate its activities with those of other Contractors. The Contractor shall clean up and remove all debris and rubbish from its work as required or directed. Upon completion of the work, the building and surrounding area of work shall be left clean and in a neat, unobstructed condition, and everything in satisfactory repair and order.

53. REPAIRED OR REPLACED PARTS / COMPONENTS

Where the Contractor is required to repair, replace or substitute Product or parts or components of the Product under the Contract, the repaired, replaced or substituted Products shall be subject to all terms and conditions for new parts and components set forth in the Contract including Warranties, as set forth in the Additional Warranties Clause herein. Replaced or repaired Product or parts and components of such Product shall be new and shall, if available, be replaced by the original manufacturer's component or part. Remanufactured parts or components

meeting new Product standards may be permitted by the Commissioner or Authorized User. Before installation, all proposed substitutes for the original manufacturer's installed parts or components must be approved by the Authorized User. The part or component shall be equal to or of better quality than the original part or component being replaced.

54. ON-SITE STORAGE With the written approval of the Authorized User, materials, equipment or supplies may be stored at the Authorized User's site at the Contractor's sole risk.

55. EMPLOYEES, SUBCONTRACTORS & AGENTS All employees, Subcontractors or agents performing work under the Contract must be trained staff or technicians who meet or exceed the professional, technical and training qualifications set forth in the Bid Specifications or the Bid Documents, whichever is more restrictive, and must comply with all security and administrative requirements of the Authorized User. The Commissioner reserves the right to conduct a security background check or otherwise approve any employee, Subcontractor or agent furnished by Contractor and to refuse access to or require replacement of any personnel for cause based on, including but not limited to, professional, technical or training qualifications, quality of work or change in security status or non-compliance with Authorized User's security or other requirements. Such approval shall not relieve the Contractor of the obligation to perform all work in compliance with the Contract terms. The Commissioner reserves the right to reject and/or bar from the facility for cause any employee, Subcontractor, or agents of the Contractor.

56. ASSIGNMENT The Contractor shall not assign, transfer, convey, sublet, or otherwise dispose of the contract or its right, title or interest therein, or its power to execute such contract to any other person, company, firm or corporation in performance of the contract without the prior written consent of the Commissioner or Authorized User (as applicable). Failure to obtain consent to assignment from the Authorized User shall revoke and annul such Contract. Notwithstanding the foregoing, the State shall not hinder, prevent or affect assignment of money by a Contractor for the benefit of its creditors. Prior to a consent to assignment of monies becoming effective, the Contractor shall file a written notice of such monies assignment(s) with the Comptroller. Prior to a consent to assignment of a Contract, or portion thereof, becoming effective, the Contractor shall submit the request to assignment to the Commissioner and seek written agreement from the Commissioner which will be filed with the Comptroller. The Commissioner reserves the right to reject any proposed assignee in his/her discretion.

Upon notice to the Contractor, the Contract may be assigned without the consent of the Contractor to another State Agency or subdivision of the State pursuant to a governmental reorganization or assignment of functions under which the functions are transferred to a successor Agency or to another Agency that assumes OGS responsibilities for the Contract.

57. SUBCONTRACTORS AND SUPPLIERS The Commissioner reserves the right to reject any proposed Subcontractor or supplier for bona fide business reasons, which may include, but are not limited to: they are on the Department of Labor's list of companies with which New York State cannot do business; the Commissioner determines that the company is not qualified; the Commissioner determines that the company is not responsible; the company has previously provided unsatisfactory work or services; the company failed to solicit minority and women's business enterprises (M/WBE) Bidders as required by prior Contracts.

58. PERFORMANCE / BID BOND The Commissioner reserves the right to require a Bidder or Contractor to furnish without additional cost, a performance, payment or Bid bond or negotiable irrevocable

letter of credit or other form of security for the faithful performance of the Contract. Where required, such bond or other security shall be in the form prescribed by the Commissioner.

59. SUSPENSION OF WORK The Commissioner, in his/her sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, in the best interests of the Authorized User. In the event of such suspension, the Contractor will be given a formal written notice outlining the particulars of such suspension. Examples of the reason for such suspension include, but are not limited to, a budget freeze or reduction on State spending, declaration of emergency, contract compliance issues or other such circumstances. Upon issuance of such notice, the Contractor is not to accept any Purchase Orders, and shall comply with the suspension order. Activity may resume at such time as the Commissioner issues a formal written notice authorizing a resumption of performance under the Contract.

An Authorized User may issue a formal written notice for the suspension of work for which it has engaged the Contractor for reasons specified in the above paragraph. The written notice shall set forth the reason for such suspension and a copy of the written notice shall be provided to the Commissioner.

60. TERMINATION

a. For Cause: For a material breach that remains uncured for more than thirty (30) days or other specified period after written notice to the Contractor, the Contract or Purchase Order may be terminated by the Commissioner or Authorized User at the Contractor's expense where Contractor becomes unable or incapable of performing, or meeting any requirements or qualifications set forth in the Contract, or for non-performance, or upon a determination that Contractor is non-responsible. Such termination shall be upon written notice to the Contractor. In such event, the Commissioner or Authorized User may complete the contractual requirements in any manner it may deem advisable and pursue available legal or equitable remedies for breach.

b. For Convenience: By written notice, this Contract may be terminated at any time by the State for convenience upon sixty (60) days written notice or other specified period without penalty or other early termination charges due. Such termination of the Contract shall not affect any project or Purchase Order that has been issued under the Contract prior to the date of such termination. If the Contract is terminated pursuant to this subdivision, the Authorized User shall remain liable for all accrued but unpaid charges incurred through the date of the termination. Contractor shall use due diligence and provide any outstanding deliverables.

c. For Violation of the Sections 139-j and 139-k of the State Finance Law: The Commissioner reserves the right to terminate the Contract in the event it is found that the certification filed by the Bidder in accordance with Section 139-k of the State Finance Law was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise its termination right by providing written notification to the Contractor in accordance with the written notification terms of the Contract.

d. For Violation of Revised Tax Law 5a: The Commissioner reserves the right to terminate the contract in the event it is found that the certification filed by the Contractor in accordance with §5-a of the Tax Law is not timely filed during the term of the Contract or the certification furnished was intentionally false or intentionally incomplete. Upon such finding, the Commissioner may exercise its termination right by providing written notification to the Contractor.

61. SAVINGS/FORCE MAJEURE A force majeure occurrence is an event or effect that cannot be reasonably anticipated or controlled.

Force majeure includes, but is not limited to, acts of God, acts of war, acts of public enemies, strikes, fires, explosions, actions of the elements, floods, or other similar causes beyond the control of the Contractor or the Commissioner in the performance of the Contract which non-performance, by exercise of reasonable diligence, cannot be prevented. Contractor shall provide the Commissioner with written notice of any force majeure occurrence as soon as the delay is known.

Neither the Contractor nor the Commissioner shall be liable to the other for any delay in or failure of performance under the Contract due to a force majeure occurrence. Any such delay in or failure of performance shall not constitute default or give rise to any liability for damages. The existence of such causes of such delay or failure shall extend the period for performance to such extent as determined by the Contractor and the Commissioner to be necessary to enable complete performance by the Contractor if reasonable diligence is exercised after the cause of delay or failure has been removed.

Notwithstanding the above, at the discretion of the Commissioner where the delay or failure will significantly impair the value of the Contract to the State or to Authorized Users, the Commissioner may:

- a. Accept allocated performance or deliveries from the Contractor. The Contractor, however, hereby agrees to grant preferential treatment to Authorized Users with respect to Product subjected to allocation; and/or
- b. Purchase from other sources (without recourse to and by the Contractor for the costs and expenses thereof) to replace all or part of the Products which are the subject of the delay, which purchases may be deducted from the Contract quantities without penalty or liability to the State; or
- c. Terminate the Contract or the portion thereof which is subject to delays, and thereby discharge any unexecuted portion of the Contract or the relative part thereof.

In addition, the Commissioner reserves the right, in his/her sole discretion, to make an equitable adjustment in the Contract terms and/or pricing should extreme and unforeseen volatility in the marketplace affect pricing or the availability of supply. "Extreme and unforeseen volatility in the marketplace" is defined as market circumstances which meet the following criteria: (i) the volatility is due to causes outside the control of Contractor; (ii) the volatility affects the marketplace or industry, not just the particular Contract source of supply; (iii) the effect on pricing or availability of supply is substantial; and (iv) the volatility so affects Contractor's performance that continued performance of the Contract would result in a substantial loss.

62. (RESERVED)

63. DEFAULT – AUTHORIZED USER

a. **Breach of Authorized User Not Breach of Centralized Contract.** An Authorized User's breach shall not be deemed a breach of the Centralized Contract, rather it shall be deemed a breach of the Authorized User's performance under the terms and conditions of the Centralized Contract.

b. **Failure to Make Payment.** In the event a participating Authorized User fails to make payment to the Contractor for Products delivered, accepted and properly invoiced, within 60 days of such delivery and acceptance, the Contractor may, upon 10 days advance written notice to both the Commissioner and the Authorized User's purchasing official, suspend additional shipments of Product or provision of services to such entity until such time as reasonable arrangements have

been made and assurances given by such entity for current and future Contract payments.

c. **Notice of Breach.** Notwithstanding the foregoing, the Contractor shall, at least 10 days prior to declaring a breach of Contract by any Authorized User, by certified or registered mail, notify both the Commissioner and the purchasing official of the breaching Authorized User of the specific facts, circumstances and grounds upon which a breach will be declared.

d. It is understood, however, that if the Contractor's basis for declaring a breach is insufficient, the Contractor's declaration of breach and failure to service an Authorized User shall constitute a breach of its Contract and the Authorized User may thereafter seek any remedy available at law or equity.

64. (RESERVED)

65. **REMEDIES FOR BREACH** It is understood and agreed that all rights and remedies afforded below shall be in addition to all remedies or actions otherwise authorized or permitted by law:

a. **Cover/Substitute Performance** In the event of Contractor's material breach, the Commissioner may, with or without formally Bidding: (i) Purchase from other sources; or (ii) If the Commissioner is unsuccessful after making reasonable attempts, under the circumstances then existing, to timely obtain acceptable service or acquire replacement Product of equal or comparable quality, the Commissioner may acquire acceptable replacement Product of lesser or greater quality.

Such purchases may, in the discretion of the Commissioner, be deducted from the Contract quantity and payments due Contractor.

b. **Withhold Payment** In any case where a question of non-performance by Contractor arises, payment may be withheld in whole or in part at the discretion of the Commissioner. Should the amount withheld be finally paid, a cash discount originally offered may be taken as if no delay in payment had occurred.

c. **Bankruptcy** In the event that the Contractor files a petition under the U.S. Bankruptcy Code during the term of this Centralized Contract, Authorized Users may, at their discretion, make application to exercise its right to set-off against monies due the Debtor or, under the Doctrine of Recoupment, credit the Authorized User the amounts owed by the Contractor arising out of the same transactions.

d. **Reimbursement of Costs Incurred** The Contractor agrees to reimburse the Authorized User promptly for any and all additional costs and expenses incurred for acquiring acceptable services, and/or replacement Product. Should the cost of cover be less than the Contract price, the Contractor shall have no claim to the difference. The Contractor covenants and agrees that in the event suit is successfully prosecuted for any default on the part of the Contractor, all costs and expenses expended or incurred by the Authorized User in connection therewith, including reasonable attorney's fees, shall be paid by the Contractor.

Where the Contractor fails to timely deliver pursuant to the guaranteed delivery terms of the Contract, the ordering Authorized User may rent substitute equipment temporarily. Any sums expended for such rental shall, upon demand, be reimbursed to the Authorized User promptly by the Contractor or deducted by the Authorized User from payments due or to become due the Contractor on the same or another transaction.

e. **Deduction/Credit** Sums due as a result of these remedies may be deducted or offset by the Authorized User from payments due, or to become due, the Contractor on the same or another transaction. If no deduction or only a partial deduction is made in such fashion the Contractor shall pay to the Authorized User the amount of such claim or portion of the claim still outstanding, on demand. The Commissioner reserves the right to determine the disposition of any rebates, settlements, restitution, liquidated damages, etc., which arise from the administration of the Contract.

66. **ASSIGNMENT OF CLAIM** Contractor hereby assigns to the State any and all its claims for overcharges associated with this Contract which may arise under the antitrust laws of the United States, 15 USC Section 1, et. seq. and the antitrust laws of the State of New York, General Business Law Section 340, et. seq.

67. **TOXIC SUBSTANCES** Each Contractor furnishing a toxic substance as defined by Section 875 of the Labor Law, shall provide such Authorized User with not less than two copies of a material safety data sheet, which sheet shall include for each such substance the information outlined in Section 876 of the Labor Law.

Before any chemical product is used or applied on or in any building, a copy of the product label and Material Safety Data Sheet must be provided to and approved by the Authorized User agency representative.

68. **INDEPENDENT CONTRACTOR** It is understood and agreed that the legal status of the Contractor, its agents, officers and employees under this Contract is that of an independent Contractor, and in no manner shall they be deemed employees of the Authorized User, and therefore are not entitled to any of the benefits associated with such employment. The Contractor agrees, during the term of this Contract, to maintain at Contractor's expense those benefits to which its employees would otherwise be entitled by law, including health benefits, and all necessary insurance for its employees, including worker's compensation, disability and unemployment insurance, and to provide the Authorized User with certification of such insurance upon request. The Contractor remains responsible for all applicable federal, state and local taxes, and all FICA contributions.

69. **SECURITY** Contractor warrants, covenants and represents that it will comply fully with all security procedures of the Authorized User(s) in performance of the Contract including but not limited to physical, facility, documentary and cyber security rules, procedures and protocols.

70. **COOPERATION WITH THIRD PARTIES** The Contractor shall be responsible for fully cooperating with any third party, including but not limited to other Contractors or Subcontractors of the Authorized User, as necessary to ensure delivery of Product or coordination of performance of services.

71. **CONTRACT TERM - RENEWAL** In addition to any stated renewal periods in the Contract, any Contract or unit portion thereof let by the Commissioner may be extended by the Commissioner for an additional period(s) of up to one year with the written concurrence of the Contractor and Comptroller. Such extension may be exercised on a month to month basis or in other stated periods of time during the one year extension.

72. **ADDITIONAL WARRANTIES** Where Contractor, product manufacturer or service provider generally offers additional or more advantageous warranties than set forth below, Contractor shall offer or pass through any such warranties to Authorized Users. Contractor hereby warrants and represents:

a. **Product Performance** Contractor warrants and represents that Products delivered pursuant to this Contract conform to the manufacturer's specifications, performance standards and documentation, and the documentation fully describes the proper procedure for using the Products.

b. **Title and Ownership Warranty** Contractor warrants, represents and conveys (i) full ownership, clear title free of all liens, or (ii) the right to transfer or deliver perpetual license rights to any Products transferred to Authorized User under this Contract. Contractor shall be solely liable for any costs of acquisition associated therewith. Contractor fully indemnifies the Authorized User for any loss, damages or actions arising from a breach of said warranty without limitation.

c. **Contractor Compliance** Contractor represents and warrants to pay, at its sole expense, for all applicable permits, licenses, tariffs, tolls and fees to give all notices and comply with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor must establish to the satisfaction of the Commissioner that it meets or exceeds all requirements of the Bid/Contract and any applicable laws, including but not limited to, permits, insurance coverage, licensing, proof of coverage for worker's compensation, and shall provide such proof as required by the Commissioner. Failure to do so may constitute grounds for the Commissioner to cancel or suspend this Contract, in whole or in part, or to take any other action deemed necessary by the Commissioner.

d. **Product Warranty** Unless recycled or recovered materials are available in accordance with the "Recycled or Recovered Materials" clause, Product offered shall be standard new equipment, current model or most recent release of regular stock product with all parts regularly used with the type of equipment offered; and no attachment or part has been substituted or applied contrary to the manufacturer's recommendations and standard practice.

Contractor further warrants and represents that components or deliverables specified and furnished by or through Contractor shall individually, and where specified and furnished as a system, be substantially uninterrupted or error-free in operation and guaranteed against faulty material and workmanship for the warranty period, or for a minimum of one (1) year from the date of acceptance, whichever is longer ("Project warranty period"). During the Project warranty period, defects in the materials or workmanship of components or deliverables specified and furnished by or through Contractor shall be repaired or replaced by Contractor at no cost or expense to the Authorized User. Contractor shall extend the Project warranty period for individual component(s), or for the System as a whole, as applicable, by the cumulative period(s) of time, after notification, during which an individual component or the System requires servicing or replacement (down time) or is in the possession of the Contractor, its agents, officers, Subcontractors, distributors, resellers or employees ("extended warranty").

Where Contractor, the Independent Software Vendor "ISV," or other third party manufacturer markets any Project Deliverable delivered by or through Contractor with a standard commercial warranty, such standard warranty shall be in addition to, and not relieve the Contractor from, Contractor's warranty obligations during the project warranty and extended warranty period(s). Where such standard commercial warranty covers all or some of the Project warranty or extended warranty period(s), Contractor shall be responsible for the coordination during the Project warranty or extended warranty period(s) with ISV or other third party manufacturer(s) for warranty

repair or replacement of ISV or other third party manufacturer's Product.

Where Contractor, ISV or other third party manufacturer markets any Project Deliverable with a standard commercial warranty which goes beyond the Project warranty or extended warranty period(s), Contractor shall notify the Authorized User and pass through the manufacturer's standard commercial warranty to Authorized User at no additional charge; provided, however, that Contractor shall not be responsible for coordinating services under the third party extended warranty after expiration of the Project warranty and extended warranty period(s).

e. Replacement Parts Warranty If during the regular or extended warranty period's faults develop, the Contractor shall promptly repair or, upon demand, replace the defective unit or component part affected. All costs for labor and material and transportation incurred to repair or replace defective Product during the warranty period shall be borne solely by the Contractor, and the State or Authorized User shall in no event be liable or responsible therefor.

Any part of component replaced by the Contractor under the Contract warranty shall be replaced at no cost to the Authorized User and guaranteed for the greater of: a) the warranty period under paragraph (d) above; or b) if a separate warranty for that part or component is generally offered by the manufacturer, the standard commercial warranty period offered by the manufacturer for the individual part or component.

f. Virus Warranty The Contractor represents and warrants that Licensed Software contains no known viruses. Contractor is not responsible for viruses introduced at Licensee's site.

g. Date/Time Warranty Contractor warrants that Product(s) furnished pursuant to this Contract shall, when used in accordance with the Product documentation, be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) transitions, including leap year calculations. Where a Contractor proposes or an acquisition requires that specific Products must perform as a package or system, this warranty shall apply to the Products as a system.

Where Contractor is providing ongoing services, including but not limited to: i) consulting, integration, code or data conversion, ii) maintenance or support services, iii) data entry or processing, or iv) contract administration services (e.g., billing, invoicing, claim processing), Contractor warrants that services shall be provided in an accurate and timely manner without interruption, failure or error due to the inaccuracy of Contractor's business operations in processing date/time data (including, but not limited to, calculating, comparing, and sequencing) various date/time transitions, including leap year calculations. Contractor shall be responsible for damages resulting from any delays, errors or untimely performance resulting therefrom, including but not limited to the failure or untimely performance of such services.

This Date/Time Warranty shall survive beyond termination or expiration of this contract through: a) ninety (90) days or b) the Contractor's or Product manufacturer/developer's stated date/time warranty term, whichever is longer. Nothing in this warranty statement shall be construed to limit any rights or remedies otherwise available under this Contract for breach of warranty.

h. Workmanship Warranty Contract warrants that all components or deliverables specified and furnished by or through Contractor under the Project Definition/Work Order meet the completion criteria set forth in the Project Definition/Work Order and any subsequent statement(s) of work, and that services will be

provided in a workmanlike manner in accordance with industry standards.

i. Survival of Warranties All warranties contained in this Contract shall survive the termination of this Contract.

73. LEGAL COMPLIANCE Contractor represents and warrants that it shall secure all notices and comply with all laws, ordinances, rules and regulations of any governmental entity in conjunction with the performance of obligations under the Contract. Prior to award and during the Contract term and any renewals thereof, Contractor must establish to the satisfaction of the Commissioner that it meets or exceeds all requirements of the Bid and Contract and any applicable laws, including but not limited to, permits, licensing, and shall provide such proof as required by the Commissioner. Failure to comply or failure to provide proof may constitute grounds for the Commissioner to cancel or suspend the Contract, in whole or in part, or to take any other action deemed necessary by the Commissioner. Contractor also agrees to disclose information and provide affirmations and certifications to comply with Sections 139-j and 139-k of the State Finance Law.

74. INDEMNIFICATION Contractor shall be fully liable for the actions of its agents, employees, partners or Subcontractors and shall fully indemnify and save harmless the Authorized Users from suits, actions, damages and costs of every name and description relating to personal injury and damage to real or personal tangible property caused by any intentional act or negligence of Contractor, its agents, employees, partners or Subcontractors, without limitation; provided, however, that the Contractor shall not indemnify for that portion of any claim, loss or damage arising hereunder due to the negligent act or failure to act of the Authorized Users.

75. INDEMNIFICATION RELATING TO THIRD PARTY RIGHTS The Contractor will also indemnify and hold the Authorized Users harmless from and against any and all damages, expenses (including reasonable attorneys' fees), claims, judgments, liabilities and costs that may be finally assessed against the Authorized Users in any action for infringement of a United States Letter Patent, or of any copyright, trademark, trade secret or other third party proprietary right except to the extent such claims arise from the Authorized Users gross negligence or willful misconduct, provided that the State shall give Contractor: (i) prompt written notice of any action, claim or threat of infringement suit, or other suit, (ii) the opportunity to take over, settle or defend such action, claim or suit at Contractor's sole expense, and (iii) assistance in the defense of any such action at the expense of Contractor.

If usage shall be enjoined for any reason or if Contractor believes that it may be enjoined, Contractor shall have the right, at its own expense and sole discretion to take action in the following order of precedence: (i) to procure for the Authorized User the right to continue Usage (ii) to modify the service or Product so that Usage becomes non-infringing, and is of at least equal quality and performance; or (iii) to replace said service or Product or part(s) thereof, as applicable, with non-infringing service or Product of at least equal quality and performance. If the above remedies are not available, the parties shall terminate the Contract, in whole or in part as necessary and applicable, provided the Authorized User is given a refund for any amounts paid for the period during which Usage was not feasible.

The foregoing provisions as to protection from third party rights shall not apply to any infringement occasioned by modification by the Authorized User of any Product without Contractor's approval.

In the event that an action at law or in equity is commenced against the Authorized User arising out of a claim that the Authorized User's use of the service or Product under the Contract infringes any patent, copyright or proprietary right, and Contractor is of the opinion that the allegations in such action in whole or in part are not covered by the indemnification and defense provisions set forth in the Contract, Contractor shall immediately notify the Authorized User and the Office of the Attorney General in writing and shall specify to what extent Contractor believes it is obligated to defend and indemnify under the terms and conditions of the Contract. Contractor shall in such event protect the interests of the Authorized User and secure a continuance to permit the Authorized User to appear and defend its interests in cooperation with Contractor, as is appropriate, including any jurisdictional defenses the Authorized User may have. This constitutes the Authorized User's sole and exclusive remedy for patent infringement, or for infringement of any other third party proprietary right.

76. LIMITATION OF LIABILITY Except as otherwise set forth in the Indemnification Paragraphs above, the limit of liability shall be as follows:

- a. Contractor's liability for any claim, loss or liability arising out of, or connected with the Products and services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Products and services, or parts thereof forming the basis of the Authorized User's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) one million dollars (\$1,000,000), whichever is greater.
- b. The Authorized User may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Authorized User unless Contractor at the time of the presentation of claim shall demonstrate to the Authorized User's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.
- c. Notwithstanding the above, neither the Contractor nor the Authorized User shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Authorized User, the Contractor, or by others.

77. INSURANCE Contractor shall secure and maintain insurance coverage as specified in the Bid Documents and shall promptly provide documentation of specified coverages to the Authorized User. If specified, the Contractor may be required to add the Authorized User as an additional insured.

**THE FOLLOWING CLAUSES PERTAIN TO
TECHNOLOGY & NEGOTIATED CONTRACTS**

78. SOFTWARE LICENSE GRANT Where Product is acquired on a licensed basis the following shall constitute the license grant:

- a. **License Scope** Licensee is granted a non-exclusive, perpetual license to use, execute, reproduce, display, perform, or merge the Product within its business enterprise in the United States up to the maximum licensed capacity stated on the Purchase Order. Product may be accessed, used, executed, reproduced, displayed or performed up to the capacity measured by the applicable licensing unit stated on the

Purchase Order (i.e., payroll size, number of employees, CPU, MIPS, MSU, concurrent user, workstation). Licensee shall have the right to use and distribute modifications or customizations of the Product to and for use by any Authorized Users otherwise licensed to use the Product, provided that any modifications, however extensive, shall not diminish Licensor's proprietary title or interest. No license, right or interest in any trademark, trade name, or service mark is granted hereunder.

b. License Term The license term shall commence upon the License Effective Date, provided, however, that where an acceptance or trial period applies to the Product, the License Term shall be extended by the time period for testing, acceptance or trial.

c. Licensed Documentation If commercially available, Licensee shall have the option to require the Contractor to deliver, at Contractor's expense: (i) one (1) hard copy and one (1) master electronic copy of the Documentation in a mutually agreeable format; (ii) based on hard copy instructions for access by downloading from the Internet (iii) hard copies of the Product Documentation by type of license in the following amounts, unless otherwise mutually agreed:

- Individual/Named User License - one (1) copy per License
- Concurrent Users - 10 copies per site
- Processing Capacity - 10 copies per site

Software media must be in a format specified by the Authorized User, without requiring any type of conversion.

Contractor hereby grants to Licensee a perpetual license right to make, reproduce (including downloading electronic copies of the Product) and distribute, either electronically or otherwise, copies of Product Documentation as necessary to enjoy full use of the Product in accordance with the terms of license.

d. Product Technical Support & Maintenance Licensee shall have the option of electing the Product technical support and maintenance ("maintenance") set forth in the Contract by giving written notice to Contractor any time during the Centralized Contract term. Maintenance term(s) and any renewal(s) thereof are independent of the expiration of the Centralized Contract term and will not automatically renew.

Maintenance shall include, at a minimum, (i) the provision of error corrections, updates, revisions, fixes, upgrade and new releases to Licensee, and (ii) Help Desk assistance with locally accessible "800" or toll free, local telephone service, or alternatively on-line Help Desk accessibility. Contractor shall maintain the Products so as to provide Licensee with the ability to utilize the Products in accordance with the Product documentation without significant functional downtime to its ongoing business operations during the maintenance term.

Authorized User shall not be required to purchase maintenance for use of Product, and may discontinue maintenance at the end of any current maintenance term upon notice to Contractor. In the event that Authorized User does not initially acquire or discontinues maintenance of licensed Product, it may, at any time thereafter, reinstate maintenance for Product without any additional penalties or other charges, by paying Contractor the amount which would have been due under the Contract for the period of time that such maintenance had lapsed, at then current NYS net maintenance rates.

e. Permitted License Transfers As Licensee's business operations may be altered, expanded or diminished, licenses granted hereunder may be transferred or combined for use at an alternative or

consolidated site not originally specified in the license, including transfers between Agencies (“permitted license transfers”). Licensee(s) do not have to obtain the approval of Contractor for permitted license transfers, but must give thirty (30) days prior written notice to Contractor of such move(s) and certify in writing that the Product is not in use at the prior site. There shall be no additional license or other transfer fees due Contractor, provided that: i) the maximum capacity of the consolidated machine is equal to the combined individual license capacity of all licenses running at the consolidated or transferred site (e.g., named users, seats, or MIPS); or ii) if the maximum capacity of the consolidated machine is greater than the individual license capacity being transferred, a logical or physical partition or other means of restricting access will be maintained within the computer system so as to restrict use and access to the Product to that unit of licensed capacity solely dedicated to beneficial use for Licensee. In the event that the maximum capacity of the consolidated machine is greater than the combined individual license capacity of all licenses running at the consolidated or transferred site, and a logical or physical partition or other means of restricting use is not available, the fees due Contractor shall not exceed the fees otherwise payable for a single license for the upgrade capacity.

f. Restricted Use By Outsourcers / Facilities Management, Service Bureaus / or Other Third Parties Outsourcers, facilities management or service bureaus retained by Licensee shall have the right to use the Product to maintain Licensee’s business operations, including data processing, for the time period that they are engaged in such activities, provided that: 1) Licensee gives notice to Contractor of such party, site of intended use of the Product, and means of access; and 2) such party has executed, or agrees to execute, the Product manufacturer’s standard nondisclosure or restricted use agreement which executed agreement shall be accepted by the Contractor (“Non-Disclosure Agreement”); and 3) if such party is engaged in the business of facility management, outsourcing, service bureau or other services, such third party will maintain a logical or physical partition within its computer system so as to restrict use and access to the program to that portion solely dedicated to beneficial use for Licensee. In no event shall Licensee assume any liability for third party’s compliance with the terms of the Non-Disclosure Agreement, nor shall the Non-Disclosure Agreement create or impose any liabilities on the State or Licensee.

Any third party with whom a Licensee has a relationship for a state function or business operation, shall have the temporary right to use Product (e.g., JAVA Applets), provided that such use shall be limited to the time period during which the third party is using the Product for the function or business activity.

g. Archival Back-Up and Disaster Recovery Licensee may use and copy the Product and related Documentation in connection with: i) reproducing a reasonable number of copies of the Product for archival backup and disaster recovery procedures in the event of destruction or corruption of the Product or disasters or emergencies which require Licensee to restore backup(s) or to initiate disaster recovery procedures for its platform or operating systems; ii) reproducing a reasonable number of copies of the Product and related Documentation for cold site storage. “Cold Site” storage shall be defined as a restorable back-up copy of the Product not to be installed until and after the declaration by the Licensee of a disaster; iii) reproducing a back-up copy of the Product to run for a reasonable period of time in conjunction with a documented consolidation or transfer otherwise allowed herein. “Disaster Recovery” shall be defined as the installation and storage of Product in ready-to-execute, back-up computer systems prior to disaster or breakdown which is not used for active production or development.

h. Confidentiality Restrictions The Product is a trade secret, copyrighted and proprietary product. Licensee and its employees will keep the Product strictly confidential, and Licensee will not disclose or otherwise distribute or reproduce any Product to anyone other than as authorized under the terms of Contract. Licensee will not remove or destroy any proprietary markings of Contractor.

i. Restricted Use by Licensee Except as expressly authorized by the terms of license, Licensee shall not:

- (i) Copy the Product;
- (ii) Cause or permit reverse compilation or reverse assembly of all or any portion of the Product;
- (iii) Export the Licensed Software in violation of any U.S. Department of Commerce export administration regulations.

79. PRODUCT ACCEPTANCE Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User(s) shall have thirty (30) days from the date of delivery to accept hardware products and sixty (60) days from the date of delivery to accept all other Product. Where the Contractor is responsible for installation, acceptance shall be from completion of installation. Failure to provide notice of acceptance or rejection or a deficiency statement to the Contractor by the end of the period provided for under this clause constitutes acceptance by the Authorized User(s) as of the expiration of that period. The License Term shall be extended by the time periods allowed for trial use, testing and acceptance unless the Commissioner or Authorized User agrees to accept the Product at completion of trial use.

Unless otherwise provided by mutual agreement of the Authorized User and the Contractor, Authorized User shall have the option to run testing on the Product prior to acceptance, such tests and data sets to be specified by User. Where using its own data or tests, Authorized User must have the tests or representative set of data available upon delivery. This demonstration will take the form of a documented installation test, capable of observation by the Authorized User, and shall be made part of the Contractor’s standard documentation. The test data shall remain accessible to the Authorized User after completion of the test.

In the event that the documented installation test cannot be completed successfully within the specified acceptance period, and the Contractor or Product is responsible for the delay, Authorized User shall have the option to cancel the order in whole or in part, or to extend the testing period for an additional thirty (30) day increment. Authorized User shall notify Contractor of acceptance upon successful completion of the documented installation test. Such cancellation shall not give rise to any cause of action against the Authorized User for damages, loss of profits, expenses, or other remuneration of any kind.

If the Authorized User elects to provide a deficiency statement specifying how the Product fails to meet the specifications within the testing period, Contractor shall have thirty (30) days to correct the deficiency, and the Authorized User shall have an additional sixty (60) days to evaluate the Product as provided herein. If the Product does not meet the specifications at the end of the extended testing period, Authorized User, upon prior written notice to Contractor, may then reject the Product and return all defective Product to Contractor, and Contractor shall refund any monies paid by the Authorized User to Contractor therefor. Costs and liabilities associated with a failure of the Product to perform in accordance with the functionality tests or product specifications during the acceptance period shall be borne fully by Contractor to the extent that said costs or liabilities shall not have been caused by negligent or willful acts or omissions of the Authorized User’s agents or employees. Said costs shall be limited to

the amounts set forth in the Limitation of Liability Clause for any liability for costs incurred at the direction or recommendation of Contractor.

80. AUDIT OF LICENSED PRODUCT USAGE Contractor shall have the right to periodically audit, no more than annually, at Contractor's expense, use of licensed Product at any site where a copy of the Product resides provided that: (i) Contractor gives Licensee(s) at least thirty (30) days advance written notice, (ii) such audit is conducted during such party's normal business hours, (iii) the audit is conducted by an independent auditor chosen on mutual agreement of the parties. Contractor shall recommend a minimum of three (3) auditing/accounting firms from which the Licensee will select one (1). In no case shall the Business Software Alliance (BSA), Software Publishers Association (SPA), Software and Industry Information Association (SIIA) or Federation Against Software Theft (FAST) be used directly or indirectly to conduct audits, or be recommended by Contractor; (iv) Contractor and Licensee are each entitled to designate a representative who shall be entitled to participate, and who shall mutually agree on audit format, and simultaneously review all information obtained by the audit. Such representatives also shall be entitled to copies of all reports, data or information obtained from the audit; and (v) if the audit shows that such party is not in compliance, Licensee shall be required to purchase additional licenses or capacities necessary to bring it into compliance and shall pay for the unlicensed capacity at the NYS Net Price in effect at time of audit, or if none, then at the Contractor's U.S. Commercial list price. Once such additional licenses or capacities are purchased, Licensee shall be deemed to have been in compliance retroactively, and Licensee shall have no further liability of any kind for the unauthorized use of the software.

81. OWNERSHIP/TITLE TO PROJECT DELIVERABLES

a. Definitions

(i) For purposes of this paragraph, "Products." A deliverable furnished under this Contract by or through Contractor, including existing and custom Products, including, but not limited to: a) components of the hardware environment, b) printed materials (including but not limited to training manuals, system and user documentation, reports, drawings), whether printed in hard copy or maintained on diskette, CD, DVD or other electronic media c) third party software, d) modifications, customizations, custom programs, program listings, programming tools, data, modules, components, and e) any properties embodied therein, whether in tangible or intangible form (including but not limited to utilities, interfaces, templates, subroutines, algorithms, formulas, source code, object code).

(ii) For purposes of this paragraph, "Existing Products." Tangible Products and intangible licensed Products that exist prior to the commencement of work under the Contract. Contractor bears the burden of proving that a particular product was in existence prior to the commencement of the Project.

(iii) For purposes of this paragraph, "Custom Products." Products, preliminary, final or otherwise, which are created or developed by Contractor, its Subcontractors, partners, employees or agents for Authorized User under the Contract.

b. Title to Project Deliverables Contractor acknowledges that it is commissioned by the Authorized User to perform the services detailed in the Purchase Order. Unless otherwise specified in writing in the Bid or Purchase Order, the Authorized User shall have ownership and license rights as follows:

(i) Existing Products:

1. Hardware - Title and ownership of Existing Hardware Product shall pass to Authorized User upon Acceptance.

2. Software - Title and ownership to Existing Software Product(s) delivered by Contractor under the Contract that is normally commercially distributed on a license basis by the Contractor or other independent software vendor proprietary owner ("Existing Licensed Product"), whether or not embedded in, delivered or operating in conjunction with hardware or Custom Products, shall remain with Contractor or the proprietary owner of other independent software vendor(s) (ISV). Effective upon acceptance, such Product shall be licensed to Authorized User in accordance with the Contractor or ISV owner's standard license agreement, provided, however, that such standard license, must, at a minimum: (a) grant Authorized User a non-exclusive, perpetual license to use, execute, reproduce, display, perform, adapt (unless Contractor advises Authorized User as part of Contractor's proposal that adaptation will violate existing agreements or statutes and Contractor demonstrates such to the Authorized User's satisfaction) and distribute Existing Licensed Product to the Authorized User up to the license capacity stated in the Purchase Order or work order with all license rights necessary to fully effect the general business purpose(s) stated in the Bid or Authorized User's Purchase Order or work order, including the financing assignment rights set forth in paragraph (c) below; and (b) recognize the State of New York as the licensee where the Authorized User is a state agency, department, board, commission, office or institution. Where these rights are not otherwise covered by the ISV's owner's standard license agreement, the Contractor shall be responsible for obtaining these rights at its sole cost and expense. The Authorized User shall reproduce all copyright notices and any other legend of ownership on any copies authorized under this paragraph.

(ii) Custom Products: Effective upon creation of Custom Products, Contractor hereby conveys, assigns and transfers to Authorized User the sole and exclusive rights, title and interest in Custom Product(s), whether preliminary, final or otherwise, including all trademark and copyrights. Contractor hereby agrees to take all necessary and appropriate steps to ensure that the Custom Products are protected against unauthorized copying, reproduction and marketing by or through Contractor, its agents, employees, or Subcontractors. Nothing herein shall preclude the Contractor from otherwise using the related or underlying general knowledge, skills, ideas, concepts, techniques and experience developed under a Purchase Order, project definition or work order in the course of Contractor's business. Authorized User may, by providing written notice thereof to the Contractor, elect in the alternative to take a non-exclusive perpetual license to Custom Products in lieu of Authorized User taking exclusive ownership and title to such Products. In such case, Licensee on behalf of all Authorized Users shall be granted a non-exclusive perpetual license to use, execute, reproduce, display, perform, adapt and distribute Custom Product as necessary to fully effect the general business purpose(s) as stated in paragraph (b)(i)(2), above.

c. Transfers or Assignments to a Third Party Financing Agent It is understood and agreed by the parties that a condition precedent to the consummation of the purchase (s) under the Contract may be the obtaining of acceptable third party financing by the Authorized User. The Authorized User shall make the sole determination of the acceptability of any financing proposal. The Authorized User will make all reasonable efforts to obtain such financing, but makes no representation that such financing has been obtained as of the date of Bid receipt. Where financing is used, Authorized User may assign or transfer its rights in Licensed Products (existing or custom) to a third party financing entity or trustee ("Trustee") as collateral where required by the terms of the financing agreement. Trustee's sole rights with respect to transferability or use of Licensed Products shall be to exclusively sublicense to Authorized User all of its Licensee's rights under the terms and conditions of the License Agreement; provided, further, however, in the event of any termination or expiration of such

sublicense by reason of payment in full, all of Trustee's rights in such Licensed Product shall terminate immediately and Authorized User's prior rights to such Existing Licensed Product shall be revived.

d. Sale or License of Custom Products Involving Tax-Exempt Financing (i.e., Certificates of Participation - COPS) The Authorized User's sale or other transfer of Custom Products which were acquired by the Authorized User using third party, tax-exempt financing may not occur until such Custom Products are, or become, useable. In the event that the Contractor wishes to obtain ownership rights to Custom Product(s), the sale or other transfer shall be at fair market value determined at the time of such sale or other transfer, and must be pursuant to a separate written agreement in a form acceptable to the Authorized User which complies with the terms of this paragraph.

e. Contractor's Obligation with Regard to ISV (Third Party) Product Where Contractor furnishes Existing Licensed Product(s) as a Project Deliverable, and sufficient rights necessary to effect the purposes of this section are not otherwise provided in the Contractor or ISV's standard license agreement, Contractor shall be responsible for obtaining from the ISV third party proprietary owner/developer the rights set forth herein to the benefit of the Authorized User at Contractor's sole cost and expense.

82. PROOF OF LICENSE The Contractor must provide to each Licensee who places a Purchase Order either: (i) the Product developer's certified License Confirmation Certificates in the name of such Licensee; or (ii) a written confirmation from the Proprietary owner accepting Product invoice as proof of license. Contractor shall submit a sample certificate, or alternatively such written confirmation from the proprietary developer. Such certificates must be in a form acceptable to the Licensee.

83. PRODUCT VERSION Purchase Orders shall be deemed to reference Manufacturer's most recently released model or version of the Product at time of order, unless an earlier model or version is specifically requested in writing by Authorized User and Contractor is willing to provide such version.

84. CHANGES TO PRODUCT OR SERVICE OFFERINGS

a. Product or Service Discontinuance Where Contractor is the Product Manufacturer/Developer, and Contractor publicly announces to all U.S. customers ("date of notice") that a Product is being withdrawn from the U.S. market or that maintenance service or technical support provided by Contractor ("withdrawn support") is no longer going to be offered, Contractor shall be required to: (i) notify the Commissioner, each Licensee and each Authorized User then under contract for maintenance or technical support in writing of the intended discontinuance; and (ii) continue to offer Product or withdrawn support upon the Contract terms previously offered for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) at Authorized User's option, provided that the Authorized User is under contract for maintenance on the date of notice, either: provide the Authorized User with a Product replacement or migration path with at least equivalent functionality at no additional charge to enable Authorized User to continue use and maintenance of the Product.

In the event that the Contractor is not the Product Manufacturer, Contractor shall be required to: (i) provide the notice required under the paragraph above, to the entities described within five (5) business days of Contractor receiving notice from the Product Manufacturer, and (ii) include in such notice the period of time from the date of notice that the Product Manufacturer will continue to provide Product or withdraw support.

The provisions of this subdivision (a) shall not apply or eliminate Contractor's obligations where withdrawn support is being provided by an independent Subcontractor. In the event that such Subcontractor ceases to provide service, Contractor shall be responsible for subcontracting such service, subject to state approval, to an alternate Subcontractor.

b. Product or Service Re-Bundling In the event that Contractor is the Product manufacturer and publicly announces to all U.S. customers ("date of notice") that a Product or maintenance or technical support offering is being re-bundled in a different manner from the structure or licensing model of the prior U.S. commercial offering, Contractor shall be required to: (i) notify the State and each Authorized User in writing of the intended change; (ii) continue to provide Product or withdrawn support upon the same terms and conditions as previously offered on the then-current NYS Contract for the greater of: a) the best terms offered by Contractor to any other customer, or b) not less than twelve (12) months from the date of notice; and (iii) shall submit the proposed rebundling change to the Commissioner for approval prior to its becoming effective for the remainder of the Contract term. The provisions of this section do not apply if the Contractor is not the Product manufacturer.

85. NO HARDSTOP/PASSIVE LICENSE MONITORING

Unless an Authorized User is otherwise specifically advised to the contrary in writing at the time of order and prior to purchase, Contractor hereby warrants and represents that the Product and all Upgrades do not and will not contain any computer code that would disable the Product or Upgrades or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral, or other similar self-destruct mechanisms (sometimes referred to as "time bombs," "time locks," or "drop dead" devices) or that would permit Contractor to access the Product to cause such disablement or impairment (sometimes referred to as a "trap door" device). Contractor agrees that in the event of a breach or alleged breach of this provision that Authorized User shall not have an adequate remedy at law, including monetary damages, and that Authorized User shall consequently be entitled to seek a temporary restraining order, injunction, or other form of equitable relief against the continuance of such breach, in addition to any and all remedies to which Authorized User shall be entitled.

86. (RESERVED)

INDEX

	<u>Paragraph</u>		<u>Paragraph</u>
<u>A</u>			
Additional Warranties	72	Modification of Contract Terms	40
Advertising Results	20		
Applicability	1	<u>N</u>	
Assignment	56	No Hardstop/Passive License Monitoring	85
Assignment of Claim	66		
Audit of Licensed Product Usage	80	<u>O</u>	
		On-Site Storage	54
		Ownership/Title to Project Deliverables	81
<u>B</u>			
Bid Contents	12		
Bid Evaluation	29	<u>P</u>	
Bid Opening	7	Performance and Responsibility Qualifications	34
Bid Submission	8	Performance/Bid Bond	58
		Prevailing Wage Rates Public Works & Building Services Contracts	17
<u>C</u>			
Changes to Product or Service Offerings	84	Pricing	24
Clarification/Revisions	31	Procurement Card	27
Confidential/Trade Secret Materials	14	Product Acceptance	79
Contract Creation/Execution	38	Product Version	83
Contract Term - Renewal	71	Prompt Payment Discounts	32
Cooperation with Third Parties	70	Proof of License	82
		Purchase Orders	44
<u>D</u>			
Default - Authorized User	63	<u>Q</u>	
Definitions	5	Quantity Changes Prior to Award	36
Disqualification for Past Performance	35		
Drawings	25	<u>R</u>	
		Release of Bid Evaluation Materials	15
<u>E</u>			
Emergency Contracts	43	Remanufactured, Recycled, Recyclable or Recovered Materials	22
Employees/Subcontractors/Agents	55	Remedies for Breach	65
Ethics Compliance	3	Repaired or Replaced Product/Components	53
Expenses Prior to Contract Execution	19		
Extraneous Terms	13	<u>S</u>	
		Savings/Force Majeure	61
<u>F</u>			
Freedom of Information Law	16	Scope Changes	41
		Security	69
		Software License Grant	78
<u>G</u>			
Governing Law	2	Subcontractors and Suppliers	57
		Suspension of Work	59
<u>I</u>			
Indemnification	74	<u>T</u>	
Indemnification Relating to Third Party Rights	75	Taxes	18
Independent Contractor	68	Termination	60
Installation	52	Title and Risk of Loss	48
Insurance	77	Toxic Substances	67
International Bidding	6		
		<u>W</u>	
<u>L</u>			
Legal Compliance	73		
Limitation of Liability	76		

Craft Workers																	
Operatives																	
Laborers and Helpers																	
Service Workers																	
Totals																	

PREPARED BY (Signature):	TELEPHONE NO.:	DATE:
	EMAIL ADDRESS:	

NAME AND TITLE OF PREPARER (Print or Type):	Submit completed form to:
	<p>NYS Office of General Services</p> <p>Corning Tower, 38th Floor</p> <p>Empire State Plaza</p> <p>Albany, NY 12242</p>

General instructions: Contact the Designated Contact(s) for the solicitation if you have any questions. **All Offerors** must complete an EEO Staffing Plan (EEO 100) and submit it as part of the bid or proposal package. Where the work force to be utilized in the performance of the State contract can be separated out from the contractor's total work force, the Offeror shall complete this form only for the anticipated work force to be utilized on the State contract. Where the work force to be utilized in the performance of the State contract cannot be separated out from the contractor's total work force, the Offeror shall complete this form for the contractor's total work force. Subcontractors awarded a subcontract over \$25,000 for the construction, demolition, replacement, major repair, renovation, planning or design of real property and improvements thereon (the "Work") except where the Work is for the beneficial use of the Contractor must complete this form upon request of OGS.

Instructions for completing:

1. Enter the Solicitation Number that this report applies to along with the name and address of the Offeror.
2. Check off the appropriate box to indicate if the Offeror completing the report is the contractor or a subcontractor.
3. Check off the appropriate box to indicate if the work force being reported is just for the contract or the Offerors' total work force.
4. Enter the total work force by EEO job category.
5. Break down the total work force by gender and enter under the heading "Work force by Gender."
6. Break down the total work force by race/ethnic background and enter under the heading "Work force by Race/Ethnic Identification." Enter the name, title, phone number and email address for the person completing the form. Sign and date the form in the designated boxes.

RACE/ETHNIC IDENTIFICATION

Race/ethnic designations as used by the Equal Employment Opportunity Commission do not denote scientific definitions of anthropological origins. For the purposes of this report, an employee may be included in the group to which he or she appears to belong, identifies with, or is regarded in the community as belonging. However, no person should be counted in more than one race/ethnic group. The race/ethnic categories for this survey are:

WHITE - (Not of Hispanic origin) All persons having origins in any of the original peoples of Europe, North Africa, or the Middle East.

BLACK - A person, not of Hispanic origin, who has origins in any of the black racial groups of the original peoples of Africa.

HISPANIC - A person of Mexican, Puerto Rican, Cuban, Central or South American or other Spanish culture or origin, regardless of race.

ASIAN & PACIFIC ISLANDER - A person having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent or the Pacific Islands.

AMERICAN INDIAN OR ALASKAN NATIVE (Not of Hispanic Origin) - A person having origins in any of the original peoples of North America, and who maintains cultural identification through tribal affiliation or community recognition.



NYS OFFICE OF GENERAL SERVICES

Serving New York

MWBE UTILIZATION PLAN

Contract No.: _____

INSTRUCTIONS: This form must be submitted with any bid, proposal, response to request for qualifications or proposed negotiated contract or within a reasonable time thereafter, but prior to contract award as required in the IFB, RFP or RFQ. This Utilization Plan must contain a detailed description of the supplies and/or services to be provided by each certified Minority and Women-owned Business Enterprise (MWBE) under the contract. Attach additional sheets if necessary.

Contractor's Name, Address and Telephone No.		Contract Description Location (Region)		MWBE Goals In Contract MBE _____ % WBE _____ %	
Federal Identification No.					

Certified M/WBE Subcontractors/Suppliers Name, Address, Telephone No, E-mail Address	Federal ID. No.	NYS ESD CERTIFIED		Detailed description of Work (Attach additional sheets if necessary)	Dollar Value of Subcontracts/ supplies/ services and intended performance dates of each component of the contract
		MBE	WBE		
		<input type="checkbox"/>	<input type="checkbox"/>		
		<input type="checkbox"/>	<input type="checkbox"/>		
		<input type="checkbox"/>	<input type="checkbox"/>		

IF UNABLE TO FULLY MEET THE MBE AND WBE GOALS SET FORTH IN THE CONTRACT, CONTRACTOR MUST SUBMIT A REQUEST FOR WAIVER (Form MWBE 101/BDC 333)

Submission of this form constitutes the contractor's acknowledgement and agreement to comply with the M/WBE requirements set forth under NYS Executive Law, Article 15-A and 5 NYCRR Part 142. Failure to submit complete and accurate information may result in a finding of noncompliance or rejection of the bid/proposal and/or suspension or termination of the contract.

Prepared By (Signature)		Email Address	
Name and Title of Preparer (Print or Type)		Telephone No.	Date

FOR M/WBE USE ONLY

Reviewed By			Date
Utilization Plan Approved <input type="checkbox"/> Yes <input type="checkbox"/> No			Date
Contract No.	Project No. (If applicable)	Contract Award Date	Estimated Completion Date
Notice of Deficiency Issued <input type="checkbox"/> Yes <input type="checkbox"/> No		Date	Description of Work
Notice of Acceptance Issued <input type="checkbox"/> Yes <input type="checkbox"/> No		Date	

Appendix D RMS RFP Glossary of Terms

Terms used in this document shall be defined in accordance with Appendix B, §5, *Definitions*, of this RFP, which is hereby incorporated by reference. In addition, the following definitions shall apply.

Term	Definition
28 CFR 23	The 28 Code of Federal Regulations (CFR) Part 23 is a set of standards for law enforcement agencies regarding the operation of federally funded, multijurisdictional, criminal intelligence systems. http://www.ecfr.gov/cgi-bin/text-idx?SID=d8124f3bd480ccdf138e27db1f505ed2&node=28:1.0.1.1.24&rgn=div5
Alert	A cautionary notification presented to users upon viewing a corresponding master name, vehicle, location, organization, or phone index.
AMS message	The Administrative Messaging System disseminates information within the New York State Division of State Police regarding serious or unusual incidents and/or incidents concerning Division equipment, vehicles, and personnel.
Assigned Officer	The primary officer responsible for a call for service, case, or assignment.
Assisting Officer	All other officers assisting with a call for service, case, or assignment.
Authorized User	“Authorized User” shall have the meaning set forth in State Finance Law section 163(1)(k). The centralized contract awarded as a result of this solicitation will be for use by Authorized Users, which includes, but is not limited to, New York State agencies, political subdivisions, local governments, public authorities, public school and fire districts, public and nonprofit libraries, and certain other nonpublic/nonprofit organizations. See RFP section entitled “Non-State Agencies Participation in Centralized Contracts.”
Auto populate	A method within the records management system that allows fields to be completed from previously entered data without user intervention.
Best Value	The basis for awarding all service and technology contracts to the Bidder that optimizes quality, cost and efficiency, among responsive and responsible Bidders. (State Finance Law §163 (1) (j)).
Bidder	The entity submitting a proposal in response to this RFP. Also referred to as “Vendor” or “Contractor.”
Blind Flag	A mechanism within the records management system to initiate a process without knowledge of the user who triggered said process.
Booking Process	Track the continuation of arrest process to include intake, detention, release and or transfers.
Bulletin	Temporary announcement, notice, or reminder from the agency to NYSP employees and other law enforcement agencies.
CJIS	Criminal Justice Information Services – FBI managed programs to provide timely and relevant criminal justice information to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations and activities, and other law enforcement related data.
BSC (Business Services Center)	A division of the New York State Office of General Services that serves as New York’s central office for processing HR and finance transitions on behalf of Executive State Agencies.

RFP 22798 - Appendix D – Glossary of Terms

Clery Act	Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act: 20 U.S.C. § 1092
Configuration	The ability to modify components of a COTS solution to meet requirements by utilizing features inherent to said solution. Configuration can be implemented by an end-user or system administrator without direct modification of the solution's source code and is often accomplished via a graphical user interface. Configuration may be needed to allow new entities to be added to the system (e.g. new agencies, new users, new action codes)
Conversion	Changing the format of existing RMS and ACISS data into a format that can be consumed by and stored in the new RMS.
Contract	The final version of any contractually binding agreement between the State and the Contractor relating to the subject matter of this RFP; references to the Contract include all exhibits, attachments and other documents attached thereto or incorporated therein by reference.
Contractor	The entity which has submitted a bid in response to this RFP and has been awarded a contract and has executed a Contract with the State. Also referred to as "Vendor."
Contract Term	The initial term of the Contract and any renewals and/or extensions.
COTS	Commercial Off-The-Shelf (COTS) is a term for goods available in the commercial marketplace that can be purchased and used under government contract.
CPL	Criminal Procedure Law
CTV	A numeric code representing a city, town, or village.
Custom Solution	A solution that requires the addition of third party software or development of features beyond those offered in the COTS offering.
Dashboard	The initial screen presented to a user of the records management system upon log-in.
DCJS	New York State Division of Criminal Justice Services
Deliverable	All materials, including goods, software licenses, data and documentation created during the performance or provision of Services hereunder or identified as a "Deliverable" in an applicable SOW.
Digital Signature	An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record.
Division	New York State Division of State Police
EEO	Equal Employment Opportunity.
Executive Agency	All state departments, offices or institutions but, for the purposes of this RFP, excludes the State University of New York and City University of New York. Furthermore, such term shall not include the legislature and judiciary. For the sake of clarity, the term "Executive Agency" does not include any public benefit corporation, public authority, or local government entity
Federated Search	Technology that allows the simultaneous search of multiple searchable resources. A user makes a single query request which is distributed to the search engines participating in the federation. The federated search then aggregates the results that are received from the search engines for presentation to the user.

RFP 22798 - Appendix D – Glossary of Terms

Flag	A mechanism to initiate a notification process within the records management system.
FOIL	The New York State Freedom of Information Law (Public Officers Law §87 et. seq.) which allows members of the public to access records of governmental agencies.
Forms	A hard copy or electronic document containing pre-defined fields requiring user input.
Free text field	An input field that allows the users to enter text information.
Fusion Center	Within the New York State Police, the New York State Intelligence Center (NYSIC) serves as the state Fusion Center which brings together federal, state and local agencies to analyze and share information related to terrorism and other crimes of a sensitive nature. Units within the NYSIC such as the Counter Terrorism Center, Special Investigations Unit, Financial Crimes Unit, CALEA, Electronic Surveillance Unit, Border Enforcement Teams and specific units within the New York State Police conducting confidential investigations
Import Data Type	Source of data imported to a Call For Service from CAD or TraCS.
Integrated Justice Portal	A central repository accessible via the Web that provides authorized users with secure access to public safety and criminal justice information from federal, state, and local sources.
ITS	New York State Information Technology Services
Juvenile	An individual that is younger than 16 years-of-age (<16).
LEA (Law Enforcement Agency)	The entities listed on Appendix O, “List of Law Enforcement Agencies,” are Law Enforcement Agencies for purposes of this RFP and the resulting Contract. The State reserves the right to revise the list of entities on Appendix O from time to time in its sole discretion.
Livescan	The digital fingerprint scanning and mug shot processing system utilized by the New York State Police.
Mandatory	Refers to items or information that the State has deemed that a Bidder must submit as compulsory, required and obligatory. These items or information are noted as such, or the requirements may be phrased in terms of “must” or “shall”. Mandatory requirements must be met by the Bidder for Bidder’s proposal to be considered responsive.
May	Denotes the permissive in a contract clause or specification. Refers to items or information that the State has deemed are worthy of obtaining, but not required or obligatory. Also see “Should”.
Members	Sworn employees of the New York State Police.
Migration	The act of consuming and storing data converted from the existing RMS and ACISS into the new RMS.
Municipality or Local Government	See Non-State Agencies.
Must	Denotes the imperative in a contract clause or specification. Means required - being determinative/mandatory, as well as imperative. Also see “Shall” and “Mandatory”.
MWBE	A business certified with Empire State Development (ESD) as a Minority and/or Woman-Owned Business.
Narrative	A free text field that allows users to document an array of police functions.
NCIC	National Crime Information Center – a CJIS service area - a computerized information system established as a service to criminal justice agencies--local, state, and federal which includes the entry, update and inquiry of person information (e.g – wanted, missing, unidentified); stolen property information and criminal history information nationwide and in Canada.
N-DEx / NY-Dex	National Law Enforcement Data Exchange / New York Data Exchange – N-DEx is a CJIS service area, is an incident or event based information sharing system for local, state, tribal and federal law enforcement agencies which securely collects and processes crime data in support of investigations, crime analysis, law enforcement administration, strategic operations and national security

RFP 22798 - Appendix D – Glossary of Terms

	responsibilities. NY-DEx is the New York equivalent which feeds information from New York agencies to N-DEx.
NLETS	The International Justice and Public Safety Network – formerly known as National Law Enforcement Telecommunications System which securely links; law enforcement and criminal justice agencies in all 50 states; Federal Agencies; U.S. territories; Canada and Mexico. Allowing agencies to communicate with each other, access respective state/territory DMV information and share information.
Non-State Agency	Political subdivisions and other entities authorized by law to make purchases from New York State centralized contracts other than those entities that qualify as State Agencies. This includes all entities permitted to participate in centralized contracts per Appendix B, §39(b), <i>Non-State Agency Authorized Users</i> and §39(c), <i>Voluntary Extension</i> and State Finance Law Section 163(1) (k).
Notification	A message presented to users regarding non-emergency, agency specific information.
NYSP	The New York State Police
NYSP Newsroom	A website provided by The New York State Police for the posting of information on calls for service. (www.nyspnews.com).
NYSPRO	The New York State Office of General Services that is authorized by law to issue centralized, statewide contracts for use by New York State agencies, political subdivisions, schools, libraries and others authorized by law to participate in such contracts.
Offense	A transgression of the law consisting of a violation, misdemeanor, or felony.
PM	Project Manager
Property / Evidence Locker	A secure location used for the storage of lost and found property, property held for safe keeping, and property of evidentiary value.
Proposal	The complete response to this RFP submitted by a Bidder to provide the services described in the RFP
Purge	The permanent removal of a record from the records management system.
Record	Any entry made into the Records Management System, including entries relating to incidents, arrests, warrants, people, vehicles and property.
Remote Access	The ability to access the Records Management System from mobile devices.
Reporting	The ability to generate statistical / analytical documents by performing a series of mathematical and logical operations against any field, or combination of fields, from within the records management system.
RFP	Request for Proposal refers to this document, its appendices and attachments.
RMS	For the purposes of this RFP, the term “RMS” shall be defined as a Law Enforcement Records Management System.
Rosario	New York State Law (People v Rosario 9 NY2d 286) that requires the retention of any statements of a witness who will testify at trial. Examples of these statements include, forms that summarize a witness statement, a signed statement by a witness, and paperwork prepared by a testifying police officer including all notes and revisions. Do we need to elaborate further?
Sealing	Court ordered redaction of all information within a case pertaining to an arrested person.
Shall	Denotes the imperative in a contract clause or specification. Means required - being determinative/mandatory, as well as imperative. Also see “Must” and “Mandatory”.
Should	Denotes the permissive in a contract clause or specification. Refers to items or information that the State has deemed are worthy of obtaining, but not required or obligatory. Also see “May”.

RFP 22798 - Appendix D – Glossary of Terms

SOW (Statement of Work)	The description of Services and Deliverables to be provided as specified in this RFP or resulting Contract.
SFS (Statewide Financial System)	The New York State Enterprise Resource Planning (ERP) system that is Oracle’s PeopleSoft software.
State	The State of New York
State Agency or State Agencies	Shall have the same meaning as “Agency” or “Agencies” in Appendix B, §5, <i>Definitions</i> .
Station	A building where one or more members of a law enforcement agency are assigned to perform police functions.
Station Bail	A sum of money received prior to arraignment by law enforcement from an arrested person, or a representative thereof, which serves as a guarantee of said person's appearance at future court proceedings; Station Bail is subsequently turned over to the presiding court.
Statistical Analysis	Collects information for use by law enforcement administration, operations, and management to report on overall crime trends, resource allocation, and support budget requests and decisions.
Tactical Analysis	Provides information to assist law enforcement operations personnel in the identification of specific policing problems and the arrest of criminal offenders.
TraCS	A software product utilized primarily for the documentation of vehicle and traffic enforcement, accident investigations, and initial incident documentation.
Transaction	An action by a user or the system that results in the storage of new or enhanced data in the RMS.
Transition	The process of moving business operations from the existing RMS and ACISS to the new RMS.
Troop	An alphabetic code utilized by the NYSP representing a geographic location within New York State.
TZS	An alpha-numeric code representing a division installation or unit of assignment by its Troop, Zone, and Station / Unit Number.
UCR / NIBRS	Uniform Crime Report / National Incident Based Reporting System – are CJIS service areas –crime reporting programs for city, county, state and federal law enforcement which provide a nationwide view of crime based upon the submission of crime statistics collected by law enforcement throughout the country.
Vendor	An enterprise that sells goods or services. Also referred to as “Bidder” or “Contractor.”
Will	Denotes the permissive in a contract clause or specification. Also see “May.”
Work Breakdown Structure	The process of subdividing project deliverables and project work into smaller, more manageable components.
Workflow	The process of routing a record through channels from its creation to approval and final disposition.
Youthful Offender	An adjudication status granted by a NYS Court at sentencing to persons at least 16 and less than 19 years of age in the interest of justice and is meant to relieve the eligible youth from the onus of having a criminal record.
Zone	A numeric code representing a geographical area within a Troop.

Volumes

Category	2013	All to Date (1/24/14)
NYSP Sworn Members	4,564	
NYSP SJS Users	4,964	
NYSP Incidents / Calls for Service	533,969	5,389,863
Incidents from Tracs	202,577	
Incidents from CAD	89,315	
NYSP Arrests	44,460	581,123
Adult Arrests	43,561	
Juvenile Arrests	899	
NYSP Warrants (Total)	5,558	30,958
Active / Open Warrants	-	5,625
NYSP Records		
CRMS Requests	9,500	
Foil Requests	2,433	
Sealed Records	7,891 (missing Dec)	
Confidential (SIU, CNET, IAB, NYSIC)	8,611	
NYSP SJS Person Entries	515,556	5,889,586
NYSP SJS Property Entries	100,355	834,467
NYSP SJS Evidence Entries	38,938	279,500
NYSP SJS Vehicle Entries	206,616	1,888,738
NYSP SJS Business Entries	3,850	71,320
NYPTI Transmissions	15,899	114,051
Initial Transmission	10,199	68,245
Final Transmission	5,690	45,806
NYSIC Field Interview Cards (FICs)	635	
Evidence in SP Possession	100,000(est.)	
Evidence SP in the Lab system	7,500	
Evidence non-SP in the Lab system	13,500	
In car Mobile Data User (Day Shift)	750	
In car Mobile Data User (Night Shift)	350	

NYS GIS Program Office Geocoding Services

Last Updated: 1/3/2014

Background

Geocoding is the process where an input address, either manually input or bulk input from a database or other source, is transformed into a consistent standardized address and a coordinate pair location. While there is only one authoritative way of storing an address using the FGDC Address Standard (<https://www.fgdc.gov/standards/projects/FGDC-standards-projects/street-address>), many different people may enter their address differently. The NYS GIS Program Office has tried to allow for as much flexibility as possible in entering addresses which can result in an FGDC standardized address and coordinate pair location. We do this by incorporating multiple versions of address locators into multiple composite locators.

Now that the SAM project (see: <http://www.dhSES.ny.gov/ocs/streets/>) is underway and the GIS Program Office has rooftop address points in many counties, we have incorporated these authoritative address points into the composite locators. We have also added additional address locators to improve geocoding results. These locators have been optimized for speed and flexibility to return the most accurate and standardized results as often as possible. To increase the speed of geocoding addresses and also maintain the flexibility and improved results of having multiple locators within the composite, the GIS Program Office split the locators into several separate composite locators. The intent is that by geocoding against the separate composite locators in a specific sequence the best result is achieved.

For example, the first composite locator (SAM_ZipName_Composite) is made up of the following list of locators. The locators are listed in the order from best to least quality along with a brief description of the locator's source data. These six locators will generate the majority of the results when geocoding addresses.

GIS Services

The composite locators are available as web services through the following links:

Updated Composite Locators:

SAM_ZipName_Composite

http://gisservices.dhSES.ny.gov/arcgis/rest/services/Locators/SAM_composite/GeocodeServer

Fallback_Locators_Composite

http://gisservices.dhSES.ny.gov/arcgis/rest/services/Locators/fallback_composite/GeocodeServer

Developers

Developers coding against the web service should include code which returns the best response from the results returned. The locaters are numbered in the order of spatial quality. Match score should not be used to choose a result form the many that may be returned. SAM points are preferred over Navteq points, which are preferred over street segments, and so on. These locaters are designed to only return valid hits, so the actual match score is of little consequence.

Sample code included here shows the logic used in picking the best result from among the geocoding results of the multiple compound locaters. This code is a fully functioning html page.

```
<!DOCTYPE html>

<html>

<head>

  <meta name="viewport" content="initial-scale=1, maximum-scale=1, user-scalable=no">

  <title>Geocoder Example</title>

  <link rel="stylesheet" href="http://js.arcgis.com/3.8/js/dojo/dijit/themes/claro/claro.css">

  <link rel="stylesheet" href="http://js.arcgis.com/3.8/js/esri/css/esri.css">

  <style>

    #container {

      width: 647px;

      margin: 20px auto;

    }

    #map {

      width: 647px;

      height: 400px;

      margin-top: 5px;

      border: 2px solid #666;

    }

  </style>

</head>

</html>
```

```
#address-input {  
    width: 350px;  
}  
  
</style>  
  
<!-- ArcGIS JS reference guide: https://developers.arcgis.com/en/javascript/jsapi/ -->  
<script src="http://js.arcgis.com/3.8/"></script>  
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script>  
</head>  
<body class="claro">  
    <div id="container">  
        <form onSubmit="return false;">  
            <input type="text" id="address-input" value="99 Washington Ave, Albany, 12210" />  
            <button id="search-btn">Search</button>  
        </form>  
  
        <div id="map"></div>  
  
        <div id="search-results"></div>  
    </div>  
</body>  
</html>  
  
<script type="text/javascript">  
    var fallback = false; //has the fallback locator been searched  
    var map, bestCandidates;  
  
    require(  
    [  

```

```
        "esri/graphic",
        "esri/symbols/SimpleMarkerSymbol",
        "esri/tasks/locator",
        "esri/map",
        "dojo/domReady!"
    ],
    function(
        Graphic,
        SimpleMarkerSymbol,
        Locator,
        Map
    ){
        //Call the searchInit function when the search button is clicked
        $('#search-btn').click(searchInit);

        var initExtent = new esri.geometry.Extent({"xmin":-82.743, "ymin":39.634, "xmax":-68.527,
"ymax":46.068, "spatialReference":{"wkid":4326}});

        //Initialize the map
        map = new Map("map", {
            basemap: "gray",
            extent: initExtent,
            logo: false,
            showAttribution: false
        });

        function searchInit() {
            //Clear previous results
            fallback = false;
        }
    }
}
```

```
$('#search-results').html('');

map.graphics.clear();

addressSearch($('#address-input').prop('value'));
}

function addressSearch(street) {

    //Build query to be sent to the geocode service
    if(fallback == false) {

        var locator = new
Locator("http://gisservices.dhSES.ny.gov/arcgis/rest/services/Locators/SAM_composite/GeocodeServer");
    }

    else {

        var locator = new
Locator("http://gisservices.dhSES.ny.gov/arcgis/rest/services/Locators/fallback_composite/GeocodeServer");
    }

    locator.on("address-to-locations-complete", displayAddressResults);
    locator.on("error", searchError);

    var address = { "SingleLine" : street };

    locator.outSpatialReference = map.spatialReference;
    locator.addressToLocations(address, ['Loc_Name']);
}

//Callback function of the geocoding services
//prints out any results found, otherwise it displays the no results found message.
function displayAddressResults(candidates) {

    /*
```

Candidate JSON format example:

```
[
  {
    address: '99 Washington Ave Albany NY 12210',
    attributes:
      {
        Loc_Name: '2A_AP_ZipName'
      }
    location:
      {
        x: -8210815.270441663,
        y: 5259598.5370621765
      }
    score: 100
  }, ...
]
```

```
*/
```

```
//Find the highest scoring candidate(s) from the best locator
```

```
bestCandidates = findBestCandidate(candidates.addresses);
```

```
if(bestCandidates.length == 0 && fallback == false) { //If the SAM locator doesn't return
any results, search the fallback locator
```

```
  fallback = true;
```

```
  addressSearch($('#address-input').prop('value'));
```

```
}
```

```
else if(bestCandidates.length == 0 && fallback == true) { //If no results were found with
either locator
```

```
  $('#search-results').html('No Addresses Found');
```

```

    }
    else {
        if(bestCandidates.length == 1) { //If there is only one result, zoom to it
            showPoint(0);
        }
        else { //If there are multiple results print them all out
            for(var i in bestCandidates) {
                $('#search-results').append('<a href="#"
onClick="showPoint(' + i + ')">' + bestCandidates[i].address + '</a><br />');
            }
        }
    }
}

//Finds the best possible candidate or set of candidates
function findBestCandidate(candidates) {
    var validCandidates = [];
    var highScore = { score: 0, type: "99" };

    for(var i in candidates) {
        var locactor_id = candidates[i].attributes.Loc_Name.split('_')[0];

        //Take the highest scoring candidate. Candidate order of precedence is
        determined by the first two characters of the Loc_Name attribute.

        //1A being the highest, followed by 1B, 2A, 2B....
        if(candidates[i].score >= highScore.score) {
            if( locactor_id <= highScore.type ) {
                candidates[i].location.points = [ [candidates[i].location.x,
candidates[i].location.y] ];
                validCandidates.push(candidates[i]);
            }
        }
    }
}

```

```

                                highScore = { score: candidates[i].score, type: locactor_id
};
                                }
                                }
                                }

                                return validCandidates;
                                }

                                function searchError(error) {
                                    console.log(error);
                                }
});

//Add a point graphic to the map for i in bestCandidates and zoom to it
function showPoint(i) {
    //Clear previous point
    map.graphics.clear();

    //Add new point graphic to the map

    var symbol = new
esri.symbol.SimpleMarkerSymbol().setStyle(esri.symbol.SimpleMarkerSymbol.STYLE_DIAMOND).setColor(new
dojo.Color([245,122,0,1]));

    var pointGraphic = new esri.Graphic(bestCandidates[i].location, symbol, {}, false);

    map.graphics.add(pointGraphic);

    //Zoom to the point

    map.centerAndZoom(bestCandidates[i].location, 15);
}
</script>
```

GENL. 3 REV. (12/05) INFORMATION/COMPLAINT

STATE OF NEW YORK

COUNTY OF _____

COURT

OF _____

THE PEOPLE OF THE STATE OF NEW YORK

- vs. -

[INFORMATION] [COMPLAINT]

Defendant(s)

ACCUSATION

BE IT KNOWN THAT, by this [Information] [Complaint], _____, as the Complainant herein, [stationed] [residing] at _____, accuses _____, the above mentioned Defendant(s), with having committed the [traffic infraction] [violation] [misdemeanor] [felony] of _____, in violation of Section _____, Subdivision _____ of the _____ Law of the State of New York.

That on or about the _____ day of _____, 20____, at about _____ [am][pm] in the _____ of _____, County of _____, the Defendant(s) did [intentionally,] [knowingly,] [recklessly,] [with criminal negligence,] and unlawfully, _____

FACTS

The above allegations of fact are made by the Complainant herein [on direct knowledge and/or upon information and belief,] with the sources of Complainant's information and the grounds for belief being the facts contained in the attached SUPPORTING DEPOSITION(s) of _____

[WHEREFORE, Complainant prays that a Warrant be issued for the arrest of the said Defendant(s).]

-OR-

[WHEREAS, an Appearance Ticket was issued to the said Defendant(s), directing [him] [her] [them] to appear before this court at _____ [am] [pm], on the _____ day of _____, 20____.]

NOTICE

In a written instrument, any person who knowingly makes a false statement, which such person does not believe to be true, has committed a crime under the laws of the State of New York punishable as a Class A Misdemeanor. (PL § 210.45)

Affirmed under penalty of perjury
this _____ day of _____, 20____.

Subscribed and Sworn to before me
this _____ day of _____, 20____.

COMPLAINANT

[] - STRIKE OUT ANY WORDS THAT DO NOT APPLY.

Agency		ORI		NEW YORK STATE DOMESTIC INCIDENT REPORT				Sprint # (NYC)		Incident #																																																																																													
DATES	Month	Day	Year	Time (24 hrs)	Address of Occurrence			APT #	Precinct (NYC) CTV	Aided # (NYC)	Complaint #																																																																																												
	How can we safely contact you? (e.g. Name, Phone)								SAFE CONTACT INFORMATION																																																																																														
VICTIM/PARTY (P1)	Name (Last, First, M.I.) / (include aliases)							Phone		DOB	Month	Day	Year	Age	<input type="radio"/> Male <input type="radio"/> Female																																																																																								
	Street & City					APT #	Zip		If non-English language: <input type="radio"/> Spanish <input type="radio"/> Chinese <input type="radio"/> Other: _____																																																																																														
VICTIM/PARTY (P2)	Name (Last, First, M.I.) / (include aliases)							Phone		DOB	Month	Day	Year	Age	<input type="radio"/> Male <input type="radio"/> Female																																																																																								
	Street & City					APT #	Zip		If non-English language: <input type="radio"/> Spanish <input type="radio"/> Chinese <input type="radio"/> Other: _____																																																																																														
SUSPECT / PARTY (P1)	Name (Last, First, M.I.) / (include aliases)							Phone		DOB	Month	Day	Year	Age	<input type="radio"/> Male <input type="radio"/> Female																																																																																								
	Street & City					APT #	Zip		If non-English language: <input type="radio"/> Spanish <input type="radio"/> Chinese <input type="radio"/> Other: _____																																																																																														
SUSPECT / PARTY (P2)	Name (Last, First, M.I.) / (include aliases)							Phone		DOB	Month	Day	Year	Age	<input type="radio"/> Male <input type="radio"/> Female																																																																																								
	Street & City					APT #	Zip		If non-English language: <input type="radio"/> Spanish <input type="radio"/> Chinese <input type="radio"/> Other: _____																																																																																														
SUSPECT / PARTY (P3)	Name (Last, First, M.I.) / (include aliases)							Phone		DOB	Month	Day	Year	Age	<input type="radio"/> Male <input type="radio"/> Female																																																																																								
	Street & City					APT #	Zip		If non-English language: <input type="radio"/> Spanish <input type="radio"/> Chinese <input type="radio"/> Other: _____																																																																																														
SUSPECT ACTIONS	<input type="radio"/> Biting <input type="radio"/> Destroyed Property (Estimated \$ _____) <input type="radio"/> Forced Entry <input type="radio"/> Forcible Restraint <input type="radio"/> Hair Pulling <input type="radio"/> Homicide <input type="radio"/> Impaired Alcohol/Drugs <input type="radio"/> Injury to Child <input type="radio"/> Injury to Other Persons <input type="radio"/> Injury to Pet/Animal <input type="radio"/> Interference with Phone <input type="radio"/> Intimidation/Coercion <input type="radio"/> Kicking <input type="radio"/> Punching <input type="radio"/> Pushing <input type="radio"/> Sexual Assault <input type="radio"/> Shooting <input type="radio"/> Slapping <input type="radio"/> Slamming Body <input type="radio"/> Stabbing <input type="radio"/> Strangulation/"Choking" <input type="radio"/> Suicide or Attempt <input type="radio"/> Threw Items <input type="radio"/> Unwanted Contact <input type="radio"/> Verbal Abuse <input type="radio"/> Violated Visitation/ Custody Conditions <input type="radio"/> OTHER Suspect Actions: _____ <input type="radio"/> Threats: (specify) <input type="radio"/> Injure/Kill Persons <input type="radio"/> Injure/Kill Self <input type="radio"/> Injure/Kill Pet/Animal <input type="radio"/> Take Child <input type="radio"/> Destroy/Take Property <input type="radio"/> Other: _____ <input type="radio"/> Threat with weapon <input type="radio"/> Weapons used: (specify) <input type="radio"/> Blunt Object <input type="radio"/> Gun <input type="radio"/> Motor Vehicle <input type="radio"/> Sharp Instrument <input type="radio"/> Other: _____																																																																																																						
	Arrest Made? <input type="radio"/> Yes <input type="radio"/> No Arrest # _____ Reasons arrest not made on-scene: <input type="radio"/> No Offense Committed <input type="radio"/> No Probable Cause <input type="radio"/> Suspect Off-Scene <input type="radio"/> Warrant/Criminal Summons to be requested <input type="radio"/> Violation level: not in police presence (no citizen's arrest) <input type="radio"/> Other: _____																																																																																																						
OFFENSES & OP	<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th>Offenses</th> <th>Law (e.g. PL)</th> <th>Section (Sub)</th> <th>Charges Filed</th> <th colspan="10">Offenses Involved: (check all that apply) <input type="radio"/> Felony <input type="radio"/> Misdemeanor <input type="radio"/> Violation <input type="radio"/> Other (Specify) _____</th> </tr> </thead> <tbody> <tr> <td>1.</td> <td></td> <td></td> <td><input type="radio"/></td> <td>Registry Checked? <input type="radio"/> Yes <input type="radio"/> No</td> <td colspan="10">OP Court Name: _____</td> </tr> <tr> <td>2.</td> <td></td> <td></td> <td><input type="radio"/></td> <td>Order of Protection? <input type="radio"/> Yes <input type="radio"/> No</td> <td colspan="10"><input type="radio"/> Family <input type="radio"/> Criminal <input type="radio"/> Supreme</td> </tr> <tr> <td>3.</td> <td></td> <td></td> <td><input type="radio"/></td> <td>Stay Away Order? <input type="radio"/> Yes <input type="radio"/> No</td> <td colspan="10"><input type="radio"/> Out of State <input type="radio"/> Tribal</td> </tr> <tr> <td></td> <td></td> <td></td> <td><input type="radio"/></td> <td>Order Violated? <input type="radio"/> Yes <input type="radio"/> No</td> <td colspan="10">Expiration Date: _____</td> </tr> <tr> <td></td> <td></td> <td></td> <td><input type="radio"/></td> <td>Any PRIOR orders? <input type="radio"/> Yes <input type="radio"/> No</td> <td colspan="10"></td> </tr> </tbody> </table>														Offenses	Law (e.g. PL)	Section (Sub)	Charges Filed	Offenses Involved: (check all that apply) <input type="radio"/> Felony <input type="radio"/> Misdemeanor <input type="radio"/> Violation <input type="radio"/> Other (Specify) _____										1.			<input type="radio"/>	Registry Checked? <input type="radio"/> Yes <input type="radio"/> No	OP Court Name: _____										2.			<input type="radio"/>	Order of Protection? <input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Family <input type="radio"/> Criminal <input type="radio"/> Supreme										3.			<input type="radio"/>	Stay Away Order? <input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Out of State <input type="radio"/> Tribal													<input type="radio"/>	Order Violated? <input type="radio"/> Yes <input type="radio"/> No	Expiration Date: _____													<input type="radio"/>	Any PRIOR orders? <input type="radio"/> Yes <input type="radio"/> No										
	Offenses	Law (e.g. PL)	Section (Sub)	Charges Filed	Offenses Involved: (check all that apply) <input type="radio"/> Felony <input type="radio"/> Misdemeanor <input type="radio"/> Violation <input type="radio"/> Other (Specify) _____																																																																																																		
1.			<input type="radio"/>	Registry Checked? <input type="radio"/> Yes <input type="radio"/> No	OP Court Name: _____																																																																																																		
2.			<input type="radio"/>	Order of Protection? <input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Family <input type="radio"/> Criminal <input type="radio"/> Supreme																																																																																																		
3.			<input type="radio"/>	Stay Away Order? <input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> Out of State <input type="radio"/> Tribal																																																																																																		
			<input type="radio"/>	Order Violated? <input type="radio"/> Yes <input type="radio"/> No	Expiration Date: _____																																																																																																		
			<input type="radio"/>	Any PRIOR orders? <input type="radio"/> Yes <input type="radio"/> No																																																																																																			
STOP! ***** COMPLETE STATEMENT ON PAGE 2 NEXT *****																																																																																																							
INVESTIGATION	Photos Taken? <input type="radio"/> Yes <input type="radio"/> No IF YES, photos taken of: <input type="radio"/> Victim Injuries <input type="radio"/> Suspect Injuries <input type="radio"/> Other evidence collected? <input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Scene <input type="radio"/> Damaged Property <input type="radio"/> Other: _____ IF YES, describe: _____																																																																																																						
	Results of investigation and basis of action taken. (Were excited utterances, spontaneous admissions or spontaneous statements made? <input type="radio"/> Yes <input type="radio"/> No (Complete 710.30 or other form when applicable). _____ _____ _____ _____																																																																																																						
OTHER AGENCIES involved with the parties or incident (e.g. advocates, hospital, probation): _____ Is there reasonable cause to suspect a child may be the victim of abuse, neglect, maltreatment or endangerment? <input type="radio"/> Yes <input type="radio"/> No IF YES, officer must contact the NYS CHILD ABUSE HOTLINE REGISTRY # 1-800-635-1522 <input type="radio"/> Guns in House <input type="radio"/> Guns Seized <input type="radio"/> Has Permit <input type="radio"/> Permit Seized Issuing County: _____ Permit #(s): _____ Name on Permit(s): _____																																																																																																							
CONTACTS INITIATED BY POLICE: <input type="radio"/> Adult Protective Services <input type="radio"/> Child Protective Services (or ACS) <input type="radio"/> Domestic Violence Services <input type="radio"/> Firearms Licensing <input type="radio"/> Mental Health <input type="radio"/> Parole <input type="radio"/> Probation <input type="radio"/> Rape Crisis <input type="radio"/> Other Agency: _____ Date: _____ Who was notified? _____ Notified by (initial): _____																																																																																																							
Officer's Signature (& Rank) (PRINT and SIGN) _____ I.D. _____ Month _____ Day _____ Year _____ Supervisor's Signature (& Rank) (PRINT and SIGN) _____ 1. Was DIR given to the victim at the scene? <input type="radio"/> Yes <input type="radio"/> No 2. Was Victim Rights Notice given to victim? <input type="radio"/> Yes <input type="radio"/> No IF NO, give reason: _____																																																																																																							
POLICE COPY (Please make a copy for your DA's office if appropriate) NYS DOMESTIC VIOLENCE HOTLINE ENGLISH: 1-800-942-6906 SPANISH: 1-800-942-6908 3221-6/05 DCJS Copyright © 2005 by NYS DCJS																																																																																																							

IF YOU ARE THE VICTIM OF DOMESTIC VIOLENCE, THE POLICE AND COURTS CAN HELP.

What the Police Can Do:

- * Assist you with finding a safe place, a place away from the violence.
- * Inform you about how the court can help protect you from the violence.
- * Help you and your children get medical care for any injuries you received.
- * Assist you in getting necessary belongings from your home.
- * Provide you with copies of police reports about the violence.
- * File a complaint in criminal court, and tell you where your local criminal and family courts are located.

What the Courts Can Do:

- * If the person who harmed or threatened you is a relative by blood or marriage, or is someone you've had a child with, then you also have the right to take your case to family court, criminal court, or both.
- * If you and the abuser are not related, were never married or don't have a child in common, then your case can be heard only in the criminal court.
- * The forms you need are available from the family court and the criminal court.
- * The courts can decide to provide a temporary order of protection for you, your children and any witnesses who may request one.
- * The family court may appoint a lawyer to help you if the court finds that you cannot afford one.
- * The family court may order temporary child support and temporary custody of your children.

New York Law States: "If you are the victim of domestic violence, you may request that the officer assist in providing for your safety and that of your children, including providing information on how to obtain a temporary order of protection. You may also request that the officer assist you in obtaining your essential personal effects and locating and taking you, or assist in making arrangements to take you, and your children to a safe place within such officer's jurisdiction, including but not limited to a domestic violence program, a family member's or a friend's residence, or a similar place of safety. When the officer's jurisdiction is more than a single county, you may ask the officer to take you or make arrangements to take you and your children to a place of safety in the county where the incident occurred. If you or your children are in need of medical treatment, you have the right to request that the officer assist you in obtaining such medical treatment. You may request a copy of any incident reports at no cost from the law enforcement agency. You have the right to seek legal counsel of your own choosing and if you proceed in family court and if it is determined that you cannot afford an attorney, one must be appointed to represent you without cost to you." "You may ask the district attorney or a law enforcement officer to file a criminal complaint. You also have the right to file a petition in the family court when a family offense has been committed against you. You have the right to have your petition and request for an order of protection filed on the same day you appear in court, and such request must be heard that same day or the next day court is in session. Either court may issue an order of protection from conduct constituting a family offense which could include, among other provisions, an order for the respondent or defendant to stay away from you and your children. The family court may also order the payment of temporary child support and award temporary custody of your children. If the family court is not in session, you may seek immediate assistance from the criminal court in obtaining an order of protection. The forms you need to obtain an order of protection are available from the family court and the local criminal court. The resources available in this community for information relating to domestic violence, treatment of injuries, and places of safety and shelters can be accessed by calling the following 800 numbers. Filing a criminal complaint or a family court petition containing allegations that are knowingly false is a crime." (NYS Criminal Procedure Law, Section 530.11 (6))

GET HELP NOW - GET SAFE - CALL:

1-800-942-6906 (English) (24 hrs.) or 1-800-942-6908 (Spanish) (24 hrs.)
 TTY for the Hearing Impaired: **1-800-818-0656 (English) or 1-800-780-7660** (Spanish and includes a language bank to 140 different languages)

In New York City, call the all language, 24 hour Domestic Violence Hotline **1-800-621-4673 (TTY 1-800-810-7444) or 311** or call your local Domestic Violence Program

Victim Information and Notification Everyday (VINE)

Victims may receive information relating to the status and release dates of persons incarcerated in state prison or local jails in New York State. For more information on this program and how you can register, call **1-888-VINE-4NY (1-888-846-3469) from a touch-tone phone (automated system)**

New York City Court Information

<u>County</u>	<u>Criminal Court (General Information: 646-386-4500)</u>	<u>Family Court</u>	
Bronx	215 East 161 St., Bronx 718-590-2000	900 Sheridan Ave., Bronx	718-590-3318
Kings	120 Schermerhorn St., Brooklyn 718-643-3909	330 Jay St., Brooklyn, NY	347-401-9600
New York	100 Centre St., New York 646-386-4615	60 Lafayette St., New York	646-386-5200
Queens	125-01 Queens Blvd., Kew Gardens 718-520-3595	151-20 Jamaica Ave., Jamaica	718-298-0197
Richmond	67 Targee St., Staten Island 718-390-8400	100 Richmond Terrace, Staten Island	718-390-5460

To obtain court information for other areas of NYS, ask the responding officer for court numbers, consult your phone directory, or call the domestic violence hotline (phone number provided above).

SI USTED ES VÍCTIMA DE LA VIOLENCIA DOMÉSTICA, LA POLICÍA Y LAS CORTES LE PUEDEN AYUDAR**Lo que puede hacer la policía:**

- * Ayudarle a encontrar un lugar seguro, un lugar lejos de la violencia.
- * Informarle cómo la corte puede ayudar a protegerle de la violencia.
- * Ayudarle a obtener atención médica para heridas o lesiones que usted y sus hijos pudieran haber sufrido.
- * Ayudarle a sacar de su hogar las pertenencias necesarias.
- * Proveerle copias de informes de la policía sobre la violencia.
- * Presentar una querrela ante la corte criminal e informarle sobre la localización de la corte criminal y de la corte de familia en su comunidad.

Lo que pueden hacer las cortes:

- * Usted tiene derecho a presentar su caso ante la corte de familia o la corte criminal, o ante ambas cortes si la persona que le causó daño o le amenazó es su pariente consanguíneo o por matrimonio, o alguien con quien usted ha tenido hijos.
- * Su caso se puede presentar solamente ante la corte criminal si usted y quien la maltrató no tienen ningún parentesco, nunca estuvieron casados, ni tuvieron hijos.
- * Puede obtener los formularios que necesita en la corte de familia y la corte criminal.
- * Las cortes podrían proveerle una orden de protección provisional para usted, sus hijos, y cualquier testigo que así lo pida.
- * Si la corte determina que usted no puede pagar por los servicios de un abogado, la corte puede asignarle uno.
- * La corte de familia puede otorgarle manutención provisional para sus hijos, así como la custodia provisional de sus hijos.

La Ley de Nueva York establece que: "Si usted es víctima de violencia doméstica, puede pedirle al oficial de la policía que resguarde su seguridad y la de sus hijos. Incluso, puede pedirle que le proporcione información sobre cómo obtener una orden temporal de protección. Asimismo, puede solicitar que dicho oficial de la policía le ayude a obtener sus efectos personales esenciales y a localizar un lugar seguro, al igual que transportarle a usted y a sus hijos a dicho lugar, o ayudarle a hacer arreglos para obtener dicha transportación dentro de la jurisdicción de dicho oficial de la policía, incluyendo pero sin limitarse a transportación a un programa que provea servicios contra la violencia doméstica, la residencia de un miembro de su familia o la residencia de un amigo, o un lugar que sea igualmente seguro. Cuando la jurisdicción de dicho oficial de la policía abarca más de un condado, usted puede pedirle al oficial que le transporte o que haga arreglos para transportarle a usted y a sus hijos a un lugar seguro en el condado donde ocurrió el incidente. Si usted o sus hijos necesitan tratamiento médico, usted tiene derecho a solicitar que dicho oficial de la policía le ayude a obtener dicho tratamiento médico. Usted puede solicitar que la agencia policial le provea una copia gratis de cualquier informe del incidente. Usted tiene derecho a buscar y escoger su propio consejero legal y si usted procede a utilizar la corte de familia y se determina que usted no puede pagar por los servicios de un abogado, uno deberá ser designado para que le represente sin costo para usted." "Usted puede pedirle al fiscal de distrito o a un oficial de la policía que radique una querrela criminal. Usted también tiene derecho a presentar una petición ante la corte de familia cuando una ofensa de familia ha sido cometida contra usted. Usted tiene derecho a presentar dicha petición y a solicitar una orden de protección el mismo día que usted comparece ante la corte, y dicha petición debe ser vista por la corte ese mismo día, o el próximo día en que la corte esté en sesión. Cualquiera de las cortes puede expedir una orden de protección contra una conducta que constituya una ofensa de familia, la cual puede incluir entre otras disposiciones, una orden contra el demandado o acusado que le requiera permanecer lejos de usted y de sus niños. La corte de familia también puede ordenar el pago temporal de manutención para sus niños y otorgarle a usted la custodia temporal de sus niños. Si la corte de familia no está en sesión, usted puede solicitar ayuda inmediata de la corte criminal para obtener una orden de protección. Los formularios que usted necesita para obtener una orden de protección están disponibles en la corte de familia y en la corte criminal local. Para acceso a los recursos disponibles en esta comunidad que proveen información sobre violencia doméstica, tratamiento de lesiones, y lugares seguros y refugios, llame a los siguientes números gratuitos. Es un crimen radicar una querrela criminal o una petición ante la corte de familia, a sabiendas de que dicha querrela o petición contiene alegaciones falsas." (NYS Criminal Procedure Law, Section 530.11 (6))

OBTEGA AYUDA AHORA - VAYA A UN LUGAR SEGURO - LLAME AL:

1-800-942-6908 (español) (24 horas) ó 1-800-942-6906 (inglés) (24 horas)
 TTY para personas con impedimento auditivo: **1-800-818-0656 (inglés) o 1-800-780-7660 (español e incluye un banco de 140 idiomas diferentes)**

En la ciudad de Nueva York, llame al teléfono de Ayuda contra la violencia doméstica
1-800-621-4673 (servicio de TTY, aparato de telecomunicaciones para sordos **1-800-810-7444**) or **311**
 o llame a su Programa local contra la violencia doméstica

Información y Notificación Diaria Para La Víctima (VINE)

Las víctimas pueden recibir información relacionada con el estado y la fecha de excarcelación de personas encarceladas en prisiones estatales o en cárceles locales en el Estado de Nueva York.

Para más información sobre este programa y como puede registrarse, llame al
1-888-VINE-4NY (1-888-846-3469) desde un teléfono de tono (sistema automatizado)

Información de la corte de la ciudad de Nueva York**Corte criminal del condado** (Información general: 646-386-4500)

Bronx	215 East 161 St., Bronx	718-590-2000
Kings	120 Schermerhorn St., Brooklyn	718-643-3909
New York	100 Centre St., New York	646-386-4615
Queens	125-01 Queens Blvd., Kew Gardens	718-520-3595
Richmond	67 Targee St., Staten Island	718-390-8400

Corte de familia

900 Sheridan Ave., Bronx	718-590-3318
330 Jay St., Brooklyn, NY	347-401-9600
60 Lafayette St., New York	646-386-5200
151-20 Jamaica Ave., Jamaica	718-298-0197
100 Richmond Terrace, Staten Island	718-390-5460

Para obtener la información de la corte para otras áreas de NYS, pedirle al oficial de la policía que responde los números de la corte, consulte su guía de telefonos, o llame el teléfono de Ayuda contra la violencia doméstica (número de teléfono proporcionado arriba).

GENL. 15 REV. 4/85 NYSP RECEIPT AND RELEASE OF PROPERTY

- *May be handwritten.*
- *Original to Division Headquarters.*
- *Copy to Evidence Custodian, if required.*

NEW YORK STATE POLICE
RECEIPT

CASE NUMBER _____ RCN _____

TROOP _____ STATION _____ DATE _____ MEMBER'S NAME _____

DESCRIPTION OF PROPERTY

VEHICLE:	YEAR	MAKE	MODEL	STYLE	COLOR
	VIN NUMBER			PLATE NUMBER	REGISTRATION STATE

SIGNATURE

RELEASE

UNDER PENALTY OF PERJURY, I, _____ ** owner - agent of owner.*
HEREBY IDENTIFY THE PROPERTY DESCRIBED ABOVE AS THE PROPERTY BELONGING TO ** me -* _____
AND HAVING REQUESTED ITS RETURN, HEREBY ACKNOWLEDGE RECEIPT OF SUCH PROPERTY WHICH IS DELIVERED INTO MY POSSESSION BY A
POLICE OFFICER AND MEMBER OF THE NEW YORK STATE POLICE ON THE _____ DAY OF _____ 20 _____
AT _____, N.Y. I DO HEREBY RELEASE AND FOREVER DISCHARGE SAID POLICE OFFICER, THE NEW YORK
STATE POLICE AND ANY AND ALL PERSONS WHO HAVE HAD SUCH PROPERTY IN THEIR CUSTODY OR UNDER THEIR CONTROL BY REASON OF
ANY PROCEEDING OR ACTION TAKEN BY THEM FOR ITS PRESERVATION TO ITS RETURN TO ** me the owner.* OF AND FROM ALL, AND ALL
MANNER OF ACTION AND ACTIONS, CAUSE, AND CAUSES OF ACTION, SUITS, DEBTS, SUMS OF MONEY, ACCOUNTS, DAMAGES OR CLAIMS OF ANY
NATURE WHATSOEVER.

DATED AT _____, N.Y. _____, 20 _____

WITNESS

OWNER / AGENT OF OWNER

Genl. 89 (11/12)

NYSP USE OF CHEMICAL AGENT/ TASER X26**OC SPRAY****TASER X26**

Serial Number _____

SUBJECT INFORMATION

Name (Last, First, MI)		2. Sex <input type="checkbox"/> M <input type="checkbox"/> F	3. Age	4. Ht.	5. Wt.
6. Race <input type="checkbox"/> White <input type="checkbox"/> White Hispanic <input type="checkbox"/> Black <input type="checkbox"/> Black Hispanic <input type="checkbox"/> American Indian and Alaskan Native <input type="checkbox"/> Asian (Asian Indians, Chinese, Japanese, Koreans, Filipinos, Indonesians, Polynesians, and other Non-Whites) <input type="checkbox"/> Unknown		7. Condition prior to use of Force (check all that apply) <input type="checkbox"/> Combative <input type="checkbox"/> Alcohol-Influenced <input type="checkbox"/> Drug Influenced <input type="checkbox"/> Hostile <input type="checkbox"/> Suicidal <input type="checkbox"/> Mentally Ill <input type="checkbox"/> Failed to follow verbal directions <input type="checkbox"/> Other _____			
8. Arrest <input type="checkbox"/> Yes <input type="checkbox"/> No	9. Armed <input type="checkbox"/> Yes w/ _____ <input type="checkbox"/> No	10. Threatened Use of Weapon <input type="checkbox"/> Yes Describe: <input type="checkbox"/> No			
11. Injured <input type="checkbox"/> Yes <input type="checkbox"/> No	12. Injury Occurred: <input type="checkbox"/> Prior to use of Force / <input type="checkbox"/> During use of Force / <input type="checkbox"/> After use of Force Describe:				
13. Injuries (specify)		<input type="checkbox"/> EMS Notified /Responded			

MEMBER INFORMATION

14. Name (Last, First, MI)		15. Sex <input type="checkbox"/> M <input type="checkbox"/> F	16. Age	17. Ht.	18. Wt.
19. Station SP _____ TZS _____		20. Shield	21. EOD	22. Rank	
23. Injured <input type="checkbox"/> Yes <input type="checkbox"/> No	24. Injury Occurred: <input type="checkbox"/> Prior to use of Force / <input type="checkbox"/> During use of Force / <input type="checkbox"/> After use of Force Describe:				
25. Injuries (specify)					

INCIDENT INFORMATION

26. Date / /	27. Tour <input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> 1 <input type="checkbox"/> F <input type="checkbox"/> 2	28. Time AM/PM	29. Location C/T/V of _____ County _____		
30. Nature of Initial Incident		31. Situation upon arrival			
32. OC Product Brand name	33. # Bursts of OC Spray	34. Distance from Subject	35. Was OC effective <input type="checkbox"/> Yes Describe reaction: <input type="checkbox"/> No		
36. Taser X26 <input type="checkbox"/> Deployed Probe <input type="checkbox"/> Contact	37. # of Discharges	38. Distance from Subject	39. Was Taser effective? <input type="checkbox"/> Yes Describe <input type="checkbox"/> No, Was a 2 nd Cartridge Discharged? <input type="checkbox"/> Yes <input type="checkbox"/> No		
40. Taser Cartridge Serial Number		41. Spent Cartridge Disposition <input type="checkbox"/> Secured <input type="checkbox"/> Discarded	Taser X-26 Data Download (Attach) Supv. Initials _____ Date _____		
42. Names of other Members/Witnesses present at time of occurrence					
43. Additional Information (Attach additional sheets as necessary)				SJS #	
44. Name/Rank of Supervisor notified				45. AMS Message #	
46. Member Signature/Date				47. Supv. Initials	

BCI 5D (Rev. 02//08)

CONSENT WAIVER TO INTERCEPT AUDIO COMMUNICATION

I, _____, residing at, _____
hereby authorize _____, a Member of the New York State Police, and
any other Member of the New York State Police, as required,

To intercept, listen to, and record conversations between myself and other persons. This
authorization covers all communications. I further authorize the New York State Police to install
whatever equipment is necessary to accomplish the interception, overhearing and recording of
these conversations.

I understand that the evidence obtained as a result of this authorization may be used in a
criminal prosecution, and that this authorization does not grant me immunity from prosecution.

This authorization shall take effect on, _____
and valid for 30 days.

Signature: _____

Print Name: _____

Dated: _____

Member's Signature: _____

Witness (es): _____
(if applicable)

CF-8 REV 06-08

• May be typed or handwritten

NEW YORK STATE POLICE
 1220 Washington Avenue, Building 22
 Albany, New York 12226-2252

REPORT OF INCIDENT VERIFICATION

<p>NOTICE: This form is to be given to the crime victim or complainant ONLY and will serve as verification that this incident was reported to the New York State Police. The Injury, Property Damage, Property Loss (Missing or Stolen), and Associated Monetary Values indicated below represent information supplied to us by the victim, complainant, owner or representative.</p> <p>Instructions: DO NOT LIST ANY SUSPECTS OR ARRESTED PERSONS ON THIS FORM. If an Incident Report is submitted, attach this form as an enclosure. Otherwise, retain with case notes.</p>		
INVESTIGATING MEMBER	CASE NUMBER	INVESTIGATING MEMBERS TROOP & STATION
DATE REPORTED TO NYSP / /	TIME REPORTED TO NYSP	LOCATION OR ADDRESS OF REPORTED INCIDENT
VICTIM <input type="checkbox"/> COMPLAINANT <input type="checkbox"/> OWNER <input type="checkbox"/> REPRESENTATIVE of OWNER <input type="checkbox"/> (check boxes that apply) NAME AND ADDRESS: _____ _____ _____		
DATE OF INCIDENT / /	Victim/Complainant/Owner reports the following type of incident: (check boxes that apply) Injury <input type="checkbox"/> Burglary <input type="checkbox"/> Criminal Mischief <input type="checkbox"/> Larceny <input type="checkbox"/> Lost/Missing Property <input type="checkbox"/> Robbery <input type="checkbox"/>	
SYNOPSIS OF REPORT MADE BY COMPLAINANT (Check boxes that apply) Injury <input type="checkbox"/> Type of Injury: _____ Injury Sustained by: Trip/Slip/Fall <input type="checkbox"/> By Accidental Act of Other <input type="checkbox"/> Reckless/Negligent Act of Other <input type="checkbox"/> Assault <input type="checkbox"/>		
Damage <input type="checkbox"/> Type of Damage: _____ Value of damage: \$ _____		
Theft <input type="checkbox"/> Property Stolen: _____ Total Value of Property: \$ _____ List of any recovered property: _____ List of damages to recovered property: _____		
Lost/Missing Property <input type="checkbox"/> _____ Total Value of Property: \$ _____		
<p>This is a Report of Incident Verification only. This is NOT an Incident Report or Criminal Investigation Report. This Report of Incident Verification is provided to the Crime Victim, Complainant, or Owner, for Insurance Claims purposes only. A copy of the Incident Report/Criminal Investigation Report will not be released at this time.</p>		
DATE	SIGNATURE OF INVESTIGATING MEMBER	

Additional property or information should be listed on the back of this form.

NEW YORK STATE POLICE

MEMORANDUM

Troop F Station Middletown
Date March 19, 2013

To: Mr. Ray Wickenheiser, Director SP Laboratory System
From: Captain Pierce V. Gallger - BCI
Subject: **PORNOGRAPHY EVIDENCE SUBMITTED FOR DESTRUCTION**

Request destruction of the pornography evidence:

Lab Case #	Station/Case# SP - BE#	Type of Evidence Submitted	Init.
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			

October 21, 2013

Lab 27A(12/07)Drug Evidence Destruction Memo (Section 34G16-NYSP Field Manual)

Troop F Station Middletown

Date _____

To: Mr. Ray Wickenheiser, Director SP Laboratory System
From: Captain Pierce V. Gallagher - BCI
Subject: DRUG EVIDENCE SUBMITTED FOR DESTRUCTION

Lot# _____
Troop Memo# 2014-

Lab Case #	Station/Case# SP - BE#	Controlled Substance/ Suspected Drug	Amt.-Wt. /Count	Init.
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

For Laboratory and NYS Dept. Of Health BCS Use Only

Drugs listed on this form, to the best of my knowledge, are no longer evidence in any criminal proceedings. I have inspected the items and the material present represents all controlled substance material. These items were destroyed on this date in my presence:

Name: _____ Signature: _____

Date: _____ Time: _____ Badge/ID No: _____ Ph.No: _____

Certification of Destruction

The drugs listed on this form have been inspected by the undersigned and the above named items verified. Items were Destroyed this date:

Narco Investigator Sig: _____ Title: _____ Date: _____

Destruction Site: _____ Method Used: _____

END OF DOCUMENT

Approved By: Technical Lieutenant/Administration Print Date: 1/15/2014

NEW YORK STATE POLICE

MEMORANDUM

Troop F Station Middletown
Date January 18, 2013

To: Mr. Ray Wickenheiser, Director SP Laboratory System
From: Captain Pierce V. Gallagher - BCI
Subject: FIREARMS SUBMITTED FOR DESTRUCTION - LONG GUNS

Request destruction of the following firearms:

Item #	Station	Case#	Lab Case #	Caliber	Make	Model	Serial #	Init.
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
Item #	Station	Case#	Lab Case #	Caliber	Make	Model	Serial #	Init.

October 21, 2013

GENL 9 Rev. 11/11

NEW YORK STATE POLICE
SEARCH AND SEIZURE
RECEIPT AND INVENTORY

_____ COURT, _____ OF _____)
)
) SS.
)
COUNTY OF _____, N.Y.

I SWEAR THAT THE FOLLOWING IS A TRUE AND DETAILED INVENTORY OF ALL PROPERTY TAKEN BY EXECUTING POLICE OFFICERS ON THE WARRANT FILED HEREWITH.

SUBSCRIBED AND SWORN TO BEFORE ME
THIS _____ DAY OF _____ 20 _____

(SIGNATURE)

(TITLE)

(SIGNATURE OF MEMBER)

**FEDERAL BUREAU OF INVESTIGATION, UNITED STATES DEPARTMENT OF JUSTICE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, CLARKSBURG, WV 26306**

PRIVACY ACT OF 1974 (PL. 93-579) REQUIRES THAT FEDERAL, STATE, OR LOCAL AGENCIES INFORM INDIVIDUALS WHOSE SOCIAL SECURITY NUMBER IS REQUESTED WHETHER SUCH DISCLOSURE IS MANDATORY OR VOLUNTARY, BASIS OF AUTHORITY FOR SUCH SOLICITATION, AND USES WHICH WILL BE MADE OF IT.

UVENILE FINGERPRINT SUBMISSION YES <input type="checkbox"/>		DATE OF ARREST MM DD YY		ORI CONTRIBUTOR ADDRESS REPLY DESIRED? YES <input type="checkbox"/>		NY1010200 SPOL LOUDONVILLE, NY	
TREAT AS ADULT YES <input type="checkbox"/>		DATE OF OFFENSE MM DD YY		PLACE OF BIRTH (STATE OR COUNTRY)		COUNTRY OF CITIZENSHIP	
END COPY TO: (ENTER ORI)		SCARS, MARKS, TATTOOS, AND AMPUTATIONS		RESIDENCE/COMPLETE ADDRESS		CITY	STATE
MISCELLANEOUS NUMBERS		LOCAL IDENTIFICATION/REFERENCE		PHOTO AVAILABLE? YES <input type="checkbox"/>		PALM PRINTS TAKEN? YES <input type="checkbox"/>	
EMPLOYER IF U.S. GOVERNMENT, INDICATE SPECIFIC AGENCY. IF MILITARY, LIST BRANCH OF SERVICE AND SERIAL NO.				OCCUPATION			
CHARGE/CITATION				DISPOSITION 1.			
				2.			
				3.			
ADDITIONAL				ADDITIONAL			
ADDITIONAL INFORMATION/BASIS FOR CAUTION				STATE BUREAU STAMP			

LEAVE BLANK	CRIMINAL	(STAPLE HERE)				LEAVE BLANK					
		STATE USAGE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
		OFF SECOND									
		SUBMISSION	APPROXIMATE CLASS	AMPUTATION	SCAR						
TE USAGE	LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX										
NATURE OF PERSON FINGERPRINTED	SOCIAL SECURITY NO.	LEAVE BLANK									
USES/MAIDEN											
T NAME, FIRST NAME, MIDDLE NAME, SUFFIX											
1. NO.	STATE IDENTIFICATION NO.	DATE OF BIRTH	MM	DD	YY	SEX	RACE	HEIGHT	WEIGHT	EYES	HAIR
1. THUMB	2. R. INDEX	3. R. MIDDLE	4. R. RING			5. R. LITTLE					
THUMB	7. L. INDEX	8. L. MIDDLE	9. L. RING			10. L. LITTLE					

1 NYSID No.		2 Name (Last, First, Middle)			3 Criminal Justice Tracking No.					
RFP 22798		Appendix H - FBI DCJS Cards			32661860Z					
4 Street Address		5 Apt/Bldg #	6 City		7 State	8 Zip				
9 Alias or Maiden Name			10 Place of Birth (State or Country)			11 Facsimile Control No.				
12 Date of Birth	13 Age	14 Sex	15 Race	16 Ethnicity	17 Skin	18 Hair	19 Eyes	20 Height	21 Wgt	
23 Arresting Officer ID No.		24 Arresting Agency Name/ORI			25 Arrest No.		26 Local ID No. <input type="checkbox"/>			
28 Arrest Date		29 Arrest Location/Code			30 Arrest Time		31 Weapon Type			
32 Incident Date		33 Incident Location/Code			34 Arrest Type		35 Arrest Status		36 Soc Sec No.	
38 C H A R G E (S)	Law	Article & Section	Sub Section	Cls	Cat	Deg	Att	Name of Offense	Cts	NCIC
	40 Signature of Arrestee									
	41 Incident No.								42 DIR Filed <input type="checkbox"/>	

22 Contributor/ORI **NY1010200**
NYSP TROOPG HDQT

1. RT	2. RI	3. RM	4. RR	5. RL
6. LT	7. LI	8. LM	9. LR	10. LL

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY L. THUMB R. THUMB RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

INITIAL REPORT TO COURT OF CRIMINAL CASE ▲ Tear off on dotted line ▲ UCS-501 03/2001

See back for full instructions - Please print or type - Always complete items in Section 1

1. Arrest Data	1 Name (Last, First, Middle)				1a Alias or Maiden Name:				2 Criminal Justice Tracking No.	
	3 NYSID No.		4 Date of Birth (MM/DD/YYYY)		5 Arresting Officer			6 Arresting Agency ORI No.		
	7 Arrest Date		8 Arrest No.		9 Arrest Type		10 Incident Date		11 Incident Place Trial Court(s)	
	12 All Arrest Charges (Fingerprintable and Non-fingerprintable)								13 Expected Arraignment Date	
	Law	Article & Section	Sub Section	Cls	Cat	Deg	Att	Name of Offense	Cts	NCIC
	14 Arraignment Court & County								15 Arraignment Court ORI	

2. Seal	16 CPL 160.50 Seal-Arrest Agency Case Closure Prior to Arraignment				17 CPL 160.50 Seal - Prosecutor decides not to proceed with Case				
	<input type="checkbox"/> Arrest agency elects not to proceed further with the arrest. Seal arrest pursuant to CPL 160.50(3)(f).				<input type="checkbox"/> Prosecutor elects not to proceed further with the case. Seal arrest pursuant to CPL 160.50(3)(f).				
Date:	Signature of Sgt. (or higher):				Date:	Signature of Prosecutor:			

RFP 22798 - Appendix H - FBI DCJS Cards

38A C H A R G E (S)	Law	Article & Section	Sub Section	Cls	Cat	Deg	Att	Name of Offense	Cts	NCIC	11A. Facsimile Control Number	
43 Date Fingerprinted			44 Signature of Person Taking Fingerprints				45 Scars, Marks, Tattoos and other Characteristics					
46 Arresting Officer's Name						47 Command			48 Misc			

INSTRUCTIONS - Enter all dates as MM/DD/YYYY e.g. 07 28 1948.
Determining # of NYS Arrest Cards to Use: *One Local Court Jurisdiction:* Submit one NYS arrest card with all the charges included. *Multiple Local Jurisdictions:* If there is more than one crime place which results in the arrest charges being tried in multiple local court jurisdictions, arrest fingerprint cards must be done for each jurisdiction. Include only those arrest charges relating to each individual court jurisdiction.

28. **ARREST DATE** - Date defendant was taken into custody. Use original arrest date, if person is being fingerprinted as the result of a bench warrant and was not printed for original arrest.

29. **ARREST LOCATION/CODE** - Enter the correct CTV (City, Town, Village) code (ex. 0101). If CTV code is unknown, enter name and type of municipality (e.g., Albany-City).

30. **ARREST TIME** - Enter in military time, the time at which the actual arrest took place.

31. **WEAPON TYPE** - Required for PL 265 arrests. Enter pistol, knife, rifle, etc.

33. **INCIDENT LOCATION/CODE** - Enter the correct CTV (City, Town, Village) Code (ex. 0101). If CTV code is unknown, enter name and type of municipality (e.g., Albany-City).

34. **ARREST TYPE** - Enter the code which best describes the circumstances of arrest.
 01-Complaint 02-Crime In Progress 03-Warrant 04-Court Summons 05-Order of Protection

35. **ARREST STATUS** - Enter the code which best describes the disposition of arrestee after arrest processing and prior to arraignment.
 01-Held 03-Released On Own Recog(ROR) 06-Police Bail
 02-Appearance Ticket 04-Cash Bail 05-Bail Bond 07-Release to 3rd Party

37. **EXPECTED ARRAIGNMENT DATE** - Enter the date the person has been told to appear in court, or the date the arresting agency takes the person to court for arraignment.

38. **CHARGE(S)** - Enter all charges with the most serious first, as set forth in the DCJS Charge Code Manual. At least one of the charges must be a fingerprintable offense as defined in CPL Section 160.10. Enter ONLY the charges relating to a single court jurisdiction if multiple crime places are involved. If more space is needed, enter in Item 38A.

LAW - Enter law abbreviation. For example: PL - Penal Law; VTL - Vehicle & Traffic Law
ARTICLE AND SECTION NUMBER - Enter Article and Section Number of Law.
SUB-SECTION - Enter sub-section, as it appears in the DCJS Charge Code Manual. If no sub-section is present, leave blank.
CLASS - Enter class of crime - A, B, C, D, E, or U-Unclassified. In the case of an "attempted" crime, enter the class as though the crime had been completed, and enter "A" in the Attempt Code field.

CAT - Enter offense category letter: F- Felony M- Misdemeanor V - Violation I - Infraction
DEGREE - Enter degree of crime, if applicable
ATTEMPT CODE - Enter "A" for attempted crimes. "C" for all other crimes.
NAME OF OFFENSE - Enter name of offense for which individual is charged, using standard abbreviations when applicable, e.g., CR POSS CONTROLLED SUBST.
COUNTS - Enter the number of counts for each offense.
NCIC CODE - Enter the appropriate 4 digit NCIC Uniform Offense Classification Code whose literal best describes the offense committed.

39. **FBI NO.** - An identification number assigned to individuals by the Federal Bureau of Investigation (FBI). Enter if known.

41. **INCIDENT NO.** (formerly arrest agency case no.) - The number assigned by the local agency that identifies the incident or complaint. It is unique to the agency but may be shared by co-offenders.

42. **DIR FILED** - Check this box if a Domestic Incident Report was filed or will be filed.

45. **SCARS, MARKS, TATTOOS AND OTHER CHARACTERISTICS** - Using the appropriate code from the NCIC Manual, enter amputations, deformities, visible scars, marks or tattoos.

48. **MISC.** - Enter any additional information which may be helpful.

1. **NYSID NUMBER** - A unique identifier assigned to an individual by the New York State Division of Criminal Justice Services (DCJS). Enter if known.

9. **ALIAS AND/OR MAIDEN NAME** - An alias is a name in which the given and/or surname is different than the name entered in field number 2.

10. **PLACE OF BIRTH** - If USA enter 2 digit state code; if not USA enter country.

14. **SEX** - Enter "M" for Male, "F" for Female or "U" for Unknown.

15. **RACE** - Enter the racial appearance code which best describes the person's appearance.
 NOTE: If Hispanic person, enter a race category here and enter "H" in field 16.
 W - White I - American Indian or Alaskan Native O - Other
 B - Black A - Asian or Pacific Islander U - Unknown

16. **ETHNICITY** - Enter "H" for Hispanic, "N" for Not Hispanic, or "U" for Unknown.

17. **SKIN** - Enter the skin tone code for the category which best describes the person's skin color (complexion).
 ALB - Albino FAR - Fair MBR - Medium Brown YEL - Yellow
 BLK - Black LGT - Light OLV - Olive OTH - Other
 DRK - Dark LBR - Light Brown RUD - Ruddy UNK - Unknown
 DBR - Dark Brown MED - Medium SAL - Sallow

18. **HAIR** - Enter hair color code which best describes the person's hair color.
 BAL - Bald BRO - Brown SDY - Sandy OTH - Other
 BLK - Black GRY - Gray WHI - White
 BLN - Blond RED - Red XXX - Unknown

19. **EYES** - Enter the eye color which best describes the person's eye color.
 BLK - Black GRY - Gray MAR - Maroon XXX - Unknown
 BLU - Blue GRN - Green PNK - Pink OTH - Other
 BRO - Brown HAZ - Hazel MUL - Multi-colored

23. **ARRESTING OFFICER ID NO.** - Unique permanent number used by your agency to identify the arresting officer.

24. **ARRESTING AGENCY NAME/ORI** - Enter the correct arresting agency ORI and name.

25. **ARREST NO.** - The unique number assigned by the local agency to identify a specific arrest of an individual, not shared with a co-offender. See fields 26 and 41.

26. **LOCAL ID NO.** - If used, the unique number assigned to the arrestee by the arresting agency. Arrest No. will be printed on rap unless box is checked in this field.

27. **COURT OF ARRAIGNMENT** - Enter the correct ORI if known. If ORI is unknown, enter court name and geographical jurisdiction (Buffalo City Court). If a Town or Village Justice, enter the court name and jurisdiction including Town or Village and the County (TJ Guilderland, Albany Co.). If there are multiple court jurisdictions, the arresting agency must submit separate arrest fingerprint cards for each jurisdiction.

UCS-501 Reverse (Rev.03/2000)

▲ Tear off on dotted line ▲

INSTRUCTIONS FOR COMPLETION OF INITIAL REPORT TO COURT OF CRIMINAL CASE

1. Arrest Data - Arrest and Anticipated Arraignment Information Completed by Arresting Agency

General Instructions: Complete field #s 1-15 following the instructions for the specific field on the DCJS-2 Arrest F/P Card. Enter identical information on both cards (UCS-501 and DCJS-2), including all arrest charges. Arresting agencies outside of NYC should attach the UCS-501 Card to the accusatory instrument and submit both to the court of arraignment.

Specific Instructions: Enter "BW Arrest" in Field #9 Arrest Type and the original arrest date in Field #7 Arrest Date, if the arrest type is "03-warrant" on the DCJS-2 Arrest F/P Card and this is bench warrant pickup on an arrest where the arrest F/P card was not initially done. Do not submit a DCJS-2 Arrest F/P Card/UCS 501 Card if done when initially arrested (submit a DCJS-6 Inquiry F/P Card instead).

Courts: Courts submitting the UCS 540 or 540A Criminal Disposition Report (CDR) manually or electronically should ensure the criminal justice tracking number and other identifiers are entered onto the CDR as reported by the arresting agency on the UCS-501 Card. Courts using on-line systems should use the criminal justice tracking number to identify the arrest file in initialization or arraignment entry routines. Courts keep the UCS-501 Card in your case file.

2. Seal - Issuing a CPL 160.50 Sealing Order for Cases Closed Prior to Arraignment in Court

Instructions: This is a CPL 160.50 seal order which causes the DCJS and FBI arrest to be sealed. Field #16 must be completed by a Sergeant or higher rank if the arresting agency closes the case prior to arraignment. Field #17 must be completed by the prosecutor if dismissing or declining to prosecute the case prior to arraignment. If the court has the UCS-501 Card at the time determination is made to drop or close the case prior to arraignment, the court should have this section completed by the appropriate PD, SO, SP or Prosecutor. **UCS-501 Sealing Order Submission:** 1. (Arrests outside of NYC) Send to NYS Div. Criminal Justice Services, CDR Processing, 4 Tower PL, Albany NY 12203-3702; or 2. (Arrests in NYC) Give card to your borough's Criminal Court for submission to UCS/DCJS.

Electronic Ticket/Accident Reporting Specifications

(Sept. 2007)

**New York State Department of Motor Vehicles
New York State Police
New York State Office of Court Administration**

Table of Contents

Policy For Electronic Tickets and Accident Reports	3
New York State Police TraCs User Agreement	6
Certification Process	9
Post-Certification	10
Tickets	11
Ticket Algorithm	11
Data Input Schema	12
Sample TSLED XML File	15
TSLED Data Elements	20
Sample Adjudication XML File	81
Adjudication Data Elements	86
Accidents	149
Accident Report Case Number	149
Data Input Schema	150
Sample XML File	156
Accident Report Data Elements	161
Exceptions Handling	186
New York Driving License 2D Barcode Format	187
New York State Registration Barcode Format	195
Attachment A- Context Diagram	202
Attachment B- Agency and Vendor Contact Information	203
Attachment C- TraCS Local Lead Agencies	205

Policy For Electronic Tickets and Accident Reports

From
New York State Police Agencies
To
New York State Police
New York State Department of Motor Vehicles and
New York State Office of Court Administration

The New York State Police (NYSP), the New York State Department of Motor Vehicles (DMV), the Office of Court Administration (OCA) and other state and federal agencies, have developed a system for the electronic transmission of ticket and accident report data from law enforcement agencies to DMV and the courts. Data standards for ticket and accident report data have been agreed to between agencies for the electronic transfer of data and are available to participating agencies.

1. In order to be certified for participation each police agency must adhere to the following requirements. Failure to do so will result in certification being withdrawn. The police agency must:
 - a. Complete testing of their data transmission before being allowed to send accident or ticket records electronically. Each agency will be certified by DSP and DMV prior to sending live production records.
 - b. Maintain all parts of the electronic ticket and accident application under their control. The portion of the system “under agency control” includes:
 - The application conforming to the State Police, DMV and OCA data requirements (e.g. edits, violation codes, tables, ticket and accident report formats).
 - The police agency’s connection to DMV and OCA provided by the State Police.
 - The ability to receive and correct data errors identified and returned to the police agency by either the State Police or DMV.

“Maintenance” generally means support, upkeep, repair and periodic duplication or “back-up” of records in order to safeguard the data. The police agency will take reasonable measures to prevent or correct system trouble with any portion of the system “under their control”. If the police agency determines any system trouble to be under NYSP or DMV control, it will notify and work with the proper NYSP representative.

2. The police agency agrees:

- a. To abide by the applicable provisions set forth in the NY State Police TraCS User Agreement.
(NOTE: The TraCS User Agreement was developed by the State Police to cover police agencies using the TraCS application. Signing this agreement does not obligate the agency to employ the TraCS application, but it does allow the agency to transmit data using the New York State Police infrastructure.)
- b. To electronically transfer ticket data to and from DMV and the courts and to print and forward paper copies of tickets where courts are not yet ready to receive electronic data online.
- c. To have their ticket and accident application software updated in a timeframe mutually agreeable to the parties, as required by state or federal agencies or mandated by changes to state and/or federal law.
- d. To have all printed ticket and accident report forms conform to the DMV standards, and to update the forms as required in a timeframe mutually agreeable to the parties.
- e. To correct error records returned to the police agency.
- f. To manage, support and ensure security is properly implemented within their system.
- g. To ensure that records are maintained in compliance with the Driver's Privacy Protection Act (DPPA.)
- h. To designate a primary point of contact for all communication with state agencies.

3. DMV agrees:

- a. To provide police agencies or their designee with updates to edit criteria, violations codes, tables, ticket and accident forms, and changes to the NYS Vehicle and Traffic Law or to Federal laws that impact the writing of traffic tickets or collection of accident data.
- b. To provide limited telephone support to answer questions during the initial setup and transmission of data through the State Police network to the Department of Motor Vehicles.
- c. To provide program documentation:
 - Policy
 - XML
 - Edits
 - Transmission Certification Procedure
 - Contact Information

The Police Agency agrees that they have read and will abide by the above policy:

Police Agency _____

By: _____ **(signed name and title)**

(Printed name and title) _____

Date _____

Return the completed form to:

NYS Dept. of Motor Vehicles
Program Analysis
6 ESP, Room 530
Albany, New York 12228
Attention: Electronic Ticket/Accident Reporting Coordinator

New York State Police TraCs User Agreement

TraCS

USE AND DISSEMINATION AGREEMENT

Between New York State Police,
the Lead Agency _____, and
_____, herein after referred to as the “Participating Agency”

WHEREAS:

New York State Police (NYSP), working with the New York State Department of Motor Vehicles (DMV), the Governor’s Traffic Safety Committee (GTSC), the Office of Court Administration (OCA) and other state and federal agencies, has developed a system for the electronic capture of ticket and accident report data in a police vehicle environment and the electronic transfer of that data from law enforcement agencies to DMV and courts. The system is called TraCS (Traffic and Criminal Software). Ticket and accident report forms have been developed and other law enforcement forms are planned for the future. DMV and the courts have approved these forms for official use. Data standards for ticket and accident report data have been agreed to between agencies for the electronic transfer of data. NYSP has developed an infrastructure and a limited capacity for local support.

It is the intention of NYSP to provide the TraCS software to any police agency in New York free of charge, based on NYSP support staff availability and the Lead Agency’s ability to self-support.

NOW THEREFORE, in consideration of the terms and conditions herein contained, the parties agree as follows:

1. NYSP agrees to provide the current version of TraCS software (includes ticket, accident report and associated forms) to the Lead Agency at no cost to the Lead Agency.
2. This Agreement will become effective upon proper execution and will remain in effect for the duration of the program, unless sooner terminated in accordance with the provisions of this Agreement.
3. This Agreement constitutes the entire Agreement between the parties hereto with respect to the subject matter hereof and shall supersede all previous negotiations, comments and writings. It shall not be released, discharged, changed or modified except by an instrument in writing signed by a duly authorized representative of each of the parties.
4. Each agency agrees:
Maintenance
To maintain all parts of the TraCS System under their control. The portion of the system “under agency control” includes:
 - The hardware and operating system associated with the in-vehicle equipment
 - The hardware and operating system associated with the in-station TraCS computer.

- Backup & restoration of all system and production ticket and/or accident report data.

“Maintenance” generally means support, upkeep, repair and periodic duplication or “back-up” of records in order to safeguard the data. The Lead Agency will take reasonable measures to prevent or correct system trouble with any portion of the system “under their control”. If the Lead Agency determines any system trouble to be under NYSP control, it will notify and work with the proper NYSP representative.

5. The Participating Agency agrees:

1. This agreement is only for the use of TraCS by the Participating Agency. TraCS software will not be distributed beyond the Participating Agency without written approval from NYSP.
2. To abide by the provisions of the TraCS Users Agreement.
3. To not alter the form(s) and TraCS database in any way without express written approval from NYSP and DMV.
4. To not introduce custom system enhancements during the Participating Agency implementation.
5. To contact the Lead Agency for all assistance with the implementation and use of the TraCS software.
6. To support reports, queries, ticket logs and any other analysis of the ticket data.
7. To coordinate the use of TraCS with local courts. However, the State Police will coordinate the assistance and response of OCA (Office of Court Administration) and DMV personnel to attend these meetings.
8. The TraCS system will be used for data entry and the electronic transfer of ticket data to and/or from DMV and the courts and the printing of ticket forms where courts are not yet online to receive electronic data.
9. Whereas a court is not yet able to accept electronic ticket data, to be responsible for printing and forwarding ticket copies to the appropriate court unless arrangements are made with individual agencies to print their own tickets and forward them to courts not yet ready to receive electronic data.
10. To supply equipment for use with the TraCS system, with the exception of any NYSP participation in the area. NYSP agrees that all NYSP equipment will be purchased, installed and supported by NYSP unless equipment is purchased by an entity for use by all agencies within a county or region.
11. To manage, support and ensure security is properly implemented within TraCS.

6. NYSP agrees:

1. To review, prioritize and schedule change requests for inclusion in future software releases. Change requests for “bug” fixes, system enhancements, form enhancements and routine change requests such as court address changes shall be directed to NYSP. Any enhancement that requires funding will be the responsibility of the Lead Agency to obtain the necessary financing and if the enhancement benefits multiple agencies, then the State Police will attempt to also obtain funding. No matter where funding comes from, NYSP and /or its contractors will make all changes to TraCS. Once

TraCS begins statewide rollout, a TraCS steering committee shall be formed to prioritize TraCS enhancements, functionality requests, issues, etc.

2. Whereas each agency will have the opportunity to participate in the electronic transfer of data, via the NYSPIN infrastructure, to a gateway server in Albany (NYSP). This data will then be transferred to DOT, DMV, OCA, etc. for processing.

7. Both parties agree:
 1. To develop a process for forms development by New York State agencies.
 2. Representatives on the TraCS steering committee shall only be from agencies that have signed this agreement.
 3. NYSP is the sole contractor and sole contact agency with Technology Enterprise Group, approved vendor of the TraCS system.
 4. NYSP is the sole contractor with the Center for Transportation Research and Education at Iowa State University, approved vendor of the CTRE Location Tool used in the TraCS system.

IN WITNESS WHEREOF, the Participating Agency, the Lead Agency and the NYSP have executed this Agreement in triplicate:

Participating Agency _____

By: _____ **(signed name and title)**

(Printed name and title) _____

Lead Agency _____

By: _____ **(signed name and title)**

(Printed name and title) _____

New York State Police

By: _____ **(signed name and title)**

(Printed name and title) _____

Return the completed application form to:

Michael Rubinstein
New York State Police
TraCS Local Agency Coordinator
Bldg 22, 1220 Washington Ave
Albany, NY 12226-2252
518.457.7040
mrubinst@troopers.state.ny.us
www.tracs.troopers.state.ny.us

Certification Process

The following are the preliminary steps:

- DSP has received the signed user agreement
- DMV has received the signed Applicant Organization form
- DMV has received the completed Vendor Information form
- DMV has received the signed policy agreement

Once these have been completed, the certification process can start

Once the user agreement has been signed and received by the State Police, they will work with the local agency to help them set up the test/certification environment.

The first step to validation will be for the local agency to install TraCs on a local PC. This will allow the local agency to enter the same ticket or accident information in TraCs that is entered in their application and to compare the XML created by both. Once the XML is an exact match to the TraCs XML, the certification process with DSP and DMV can begin by contacting...

State Police

- Verify Communications / Firewall issues with the State police
 - Send File to State Police to test server setup and communications
 - State Police will verify results
- Validate XML data
 - State Police will manually run file through test environment
 - State Police will post errors on test web site.
- Process continues until State Police signs off

DMV

- State Police passes file to DMV for validation (DMV passes on to OCA for parallel validation.)
 - Same communication as all other file transfers
- Validation with DMV
 - Police Agency must send copies of its printed Ticket, Simplified Traffic Information /Conviction Certificate and Accident Report forms to DMV for certification.
 - DMV runs file through appropriate test process (TSLED/ADJ/Accidents)
 - DMV will communicate errors back to the State Police to be posted on the test Web site
- Process continues until DMV signs off
- Police Agency must send copies of its printed Ticket, Simplified Traffic Information /Conviction Certificate and Accident Report forms to DMV for certification.

OCA

- DMV passes file to OCA for validation
 - Same communication as all other file transfers
- Validation with OCA

- OCA runs file (minimum 25 tickets) through appropriate test process (TSLED/ADJ)
- OCA validates file against Simplified Traffic Information /Conviction Certificate (paper or .pdf)
- Process continues until OCA signs off

DOT

(Accident Reports only)

- State Police passes file to DOT for validation
 - Same communication as all other file transfers
- Validation with DOT
 - DOT runs file through appropriate test process (Accidents)
- Process continues until DOT signs off

Post-Certification

After initial certification for the transmission and acceptance of electronic tickets, the police agency will be monitored for six months and will then receive a performance evaluation. Twelve months after initial certification the police agency will again be evaluated for Re-Certification to determine if they have met the following two conditions:

- I. Acceptable Error Rate --The police agency must maintain an acceptable error rate for transmitted tickets, and for accident reports when those are transmitted. The error rate (percentage of records rejected by DMV and returned to the police agency by way of the NYSP) must be equal to or lower than 3%. Certification will be revoked if the acceptable error rate standard is not maintained.
- II. Electronic Accident Reports-- While the certification of electronic tickets may occur first, it is expected that an agency's software will be able to transmit police accident reports electronically. Certification of electronic accident reports will be expected by the time of the Re-Certification process, twelve months after the initial ticketing certification. Failure to attain certification for accident reports will result in revocation of certification for tickets.

Tickets

Ticket Algorithm

In order to prevent duplicate ticket numbers among the many TraCS agencies and locations across New York, the TraCS Universal Ticket Number is a unique 10-character value with the following components:

pos	Description
1-4	<p>Machine code-This number MUST be UNIQUE within the issuing agency as it will become part of each Ticket and Accident Report number. The Criteria for the Machine Number is as follows:</p> <ul style="list-style-type: none"> - Only letters and numbers are allowed, no special characters - All letters must be UPPER CASE - The machine number MUST be exactly 4 characters long - It can NOT start with Zero or the letter "O" - The 4th character MUST be a number - The first 3 characters of the machine number should not spell or imply anything offensive; the machine number is the first 4 characters of the Ticket number, and the third - sixth characters of the Accident Report number and as such will be seen by the public.
5-8	<p>TraCS Sequence Numbering- (Modified Base 30)</p> <ul style="list-style-type: none"> - Created by using the letters of the alphabet A-Z plus 0-9 characters minus vowels (A,E,I,O,U,Y) - Insures that the ticket will not spell or imply anything offensive - Recommend in place of using only numerics so more than 9999 tickets can be written
9-10	The agency code as assigned by DMV

Example:

Ticket Number	Machine Code	Sequence Number	Agency Code
PG12B58XNN	PG12	B58X	NN
NT40K434TW	NT40	K434	TW

Data Input Schema

The following Schema illustrates the data element input 'tags' for tickets (UTT.)

The XML Schema is also available at:

http://www.nycourts.gov/ea/XML/XML_Data/RSS/Tracs_Schema_RSS_20_Feed.xml

```

<Ticket>
  <PrdHeader>
    <TicketNumber></TicketNumber>
    <NCIC></NCIC>
    <BadgeNumber></BadgeNumber>
    <ArrestingOfficerInitials></ArrestingOfficerInitials>
    <ArrestingOfficerName>< </ArrestingOfficerName>
    <Officer_Signature></Officer_Signature>
    <TVB></TVB>
    <Radar_Officer_Signature></Radar_Officer_Signature
  </PrdHeader>
  <Motorist>
    <FirstName></FirstName>
    <MI></MI>
    <LastName></LastName>
    <Suffix></Suffix>
    <StreetAddress></StreetAddress>
    <City></City>
    <State></State>
    <ZipCode></ZipCode>
    <DateOfBirth></DateOfBirth>
    <Age></Age>
    <DateExpires></DateExpires>
    <Gender></Gender>
    <License>
      <Number></Number>
      <State></State>
      <Class></Class>
    </License>
  </Motorist>
  <Vehicle>
    <PlateNumber></PlateNumber>
    <PlateState></PlateState>
    <RegistrationType></RegistrationType>
    <VehicleType></VehicleType>
    <Make></Make>
    <Year></Year>

```

```

    <Model ></Model>
    <RegExpires></RegExpires>
    <VehColor></VehColor>
    <VIN></VIN >
    <RegisteredWeight></RegisteredWeight>
    <ActualWeight></ ActualWeight >
    <NumberOfAxles></NumberOfAxles>
    <Commercial></Commercial>
    <Bus></Bus>
    <HazardousMaterial></HazardousMaterial>
    <OwnerOwned></OwnerOwned>
    <DOTNumber></DOTNumber>
</Vehicle>
<Court>
    <Code></Code>
    <Name></Name>
    <StreetAddress></StreetAddress>
    <City></City>
    <State></State>
    <ZipCode></ZipCode>
    <CourtDate></CourtDate>
    <CourtTime></CourtTime>
    <DWITest></DWITest>
    <TestType></TestType>
    <TestResults></TestResults>
    <OfficerNotes></OfficerNotes>
    <ReturnByMail></ReturnByMail>
</Court>
<SupportingDeposition>
    <Type></Type>
    <Information></Information>
    <DefendantStatement></DefendantStatement>
    <ChargeBased></ChargeBased>
    <DirectionTravel></DirectionTravel>
</SupportingDeposition>
<Violation>
    <ViolationDate></ViolationDate>
    <TypeOfLaw></TypeOfLaw>
    <ViolationCharged></ViolationCharged>
    <ActualSpeed></ActualSpeed>
    <ZoneSpeed></ZoneSpeed>
    <HighwayTypeCode></HighwayTypeCode>
    <RouteCode></RouteCode>
    <MuniCode></MuniCode>
    <Municipality></ Municipality>
    <ArrestTypeCode></ArrestTypeCode>
    <AlcoholDrugTest></AlcoholDrugTest>
    < AlcoholDrugTestType></AlcoholDrugTestType>

```

```

<AlcoholTestResult></AlcoholTestResult>
<DrugTestResult></ DrugTestResult>

<ArrestTransactionDate></ArrestTransactionDate>
<LocalOffice></LocalOffice>
<PoliceAgency></PoliceAgency>
<CTVName></CTVName>
<PlaceOfOccurance></PlaceOfOccurance>
<DriverLicShown></DriverLicShown>
<ViolationDescription></ViolationDescription>
<LawSection></LawSection>
<Ordinal></Ordinal>
</Violation>
<Location>
  <AtIntersection></AtIntersection>
  <CaptureDate></CaptureDate>
  <DistanceType></DistanceType>
  <Intersection></Intersection>
  <LocationDefinable></LocationDefinable>
  <LocationDirection></LocationDirection>
  <LocationDistance></LocationDistance>
  <LocCounty></LocCounty>
  <LocToolVersion></LocToolVersion>
  <ReferenceMarker></ ReferenceMarker>
  <Road></Road>
  <SnapStatus></SnapStatus>
  <XCoordinate></XCoordinate>
  <YCoordinate></YCoordinate>
  <ZCoordinate></ZCoordinate>
</Location>
</Ticket>

```

Sample TSLED XML File

```

<File name="Abc_file" ID="37124">
  <Contents>
    <Ticket>
      <PrdHeader>
        <TicketNumber>
          1A110001SS
        </TicketNumber>
        <NCIC>
          13102
        </NCIC>
        <BadgeNumber>
          9999
        </BadgeNumber>
        <ArrestingOfficerInitials>
          SO
        </ArrestingOfficerInitials>
        <ArrestingOfficerName>
          SAMPLE OFFICER
        </ArrestingOfficerName>
        <OfficerSignature>
          R0IGODlh6wA3AMQAAAAAAP///wAAAAAAAAAAAA
          (Actual code representing signature is in excess of 12 lines;
          it has been abridged here to conserve page space.)
          kuSVOuHj55U0ejmnmNGaeSV+aX67JZptqDRECADs=
        </OfficerSignature>
        <TVB>
          N
        </TVB>
        <Radar_Officer_Signature>
        </Radar_Officer_Signature>
      </PrdHeader>
      <Motorist>
        <FirstName>
          SALLY
        </FirstName>
        <MI>
          D
        </MI>
        <LastName>
          SAMPLE
        </LastName>
        <Suffix>
        </Suffix>
        <StreetAddress>
          1010 ANYPLACE ST
    
```

```
</StreetAddress>
<City>
YOURCITY
</City>
<State>
NY
</State>
<ZipCode>
12121
</ZipCode>
<DateOfBirth>
7/18/1993
</DateOfBirth>
<Age>
</Age>
<DateExpires>
7/18/2013
</DateExpires>
<Gender>
F
</Gender>
<License>
    <Number>
    </Number>
    <State>
    NY
    </State>
    <Class>
    </Class>
</License>
</Motorist>
<Vehicle>
    <PlateNumber>
    123ABC
    </PlateNumber>
    <PlateState>
    NY
    </PlateState>
    <VehicleType>
    1
    </VehicleType>
    <Make>
    </Make>
    <Year>
    1997
    </Year>
    <RegExpires>
    6/30/2006
```

```
</RegExpires>
<VehColor>
BK
</VehColor>
<VIN>
</VIN>
<RegisteredWeight>
</RegisteredWeight>
<ActualWeight>
</ActualWeight>
<NumberOfAxles>
</NumberOfAxles>
<Commercial>
</Commercial>
<Bus>
</Bus>
<HazardousMaterial>
</HazardousMaterial>
<OwnerOwned>
1
</OwnerOwned>
<DOTNumber>
</DOTNumber>
</Vehicle>
<Court>
<Code>
NY031121J
</Code>
<Name>
YOUR TOWN COURT
</Name>
<StreetAddress>
</StreetAddress>
<City>
COURT CITY
</City>
<State>
NY
</State>
<ZipCode>
12345
</ZipCode>
<CourtDate>
12/27/2005
</CourtDate>
<CourtTime>
19:00
</CourtTime>
```

```

    <DWITest>
    </DWITest>
    <TestType>
    </TestType>
    <TestResults>
    </TestResults>
    <OfficerNotes>
    </OfficerNotes>
    <ReturnByMail>
    1
    </ReturnByMail>
  </Court>
  <SupportingDeposition>
    <Type>
    1
    </Type>
    <Information>
    </Information>
    <DefendantStatement>
    </DefendantStatement>
    <ChargeBased>
    </ChargeBased>
    <DirectionTravel>
    </DirectionTravel>
  </SupportingDeposition>
  <Violation>
    <ViolationDate>
    12/18/200508:01:00
    </ViolationDate>
    <TypeOfLaw>
    VTL
    </TypeOfLaw>
    <ViolationCharged>
    VTL0375 31 010
    </ViolationCharged>
    <ActualSpeed>
    000
    </ActualSpeed>
    <ZoneSpeed>
    000
    </ZoneSpeed>
    <HighwayTypeCode>
    3
    </HighwayTypeCode>
    <RouteCode>
    </RouteCode>
    <MuniCode>
    3452
  
```

```
</MuniCode>
<Municipality>
TOWN OF CLAY
</Municipality>
<ArrestTypeCode>
1
</ArrestTypeCode>
<AlcoholDrugTest>
</AlcoholDrugTest>
<AlcoholDrugTestType>
</AlcoholDrugTestType>
<AlcoholTestResult>
</AlcoholTestResult>
<DrugTestResult>
</DrugTestResult>
<ArrestTransactionDate>
12/18/200500:00:00
</ArrestTransactionDate>
<LocalOffice>
A111
</LocalOffice>
<PoliceAgency>
TOWN OF CLAY POLICE
</PoliceAgency>
<CTVName>
3452
</CTVName>
<PlaceOfOccurance>
SOULE ROAD
</PlaceOfOccurance>
<DriverLicShown>
1
</DriverLicShown>
<ViolationDescription>
INADEQUATE MUFFLER-LOUD
</ViolationDescription>
<LawSection>
37531
</LawSection>
<Ordinal>
</Ordinal>
</Violation>
<Location>
</Location>
</Ticket>
</Contents>
</File>
```

TSLED Data Elements

Description: Traffic Safety Law Enforcement and Disposition (TLSED): The following schema gives the requirements and descriptions for each data element as it is used and viewed by TSLED

Additional information may be found on the TraCS Data Element RSS feed:

http://www.nycourts.gov/ea/XML/XML_Data/RSS/Tracs_Schema_RSS_20_Feed.xml

<File name="" ID="">

Description: **Ticket File**

Restrictions:

Attributes for: <File> Element (NYSP creates the file element (Name and ID.) Do not include this element in your files.)

Attribute Name: **name**

Description: **File name**

Sample data: **Abc_file**

Restrictions: **Data must adhere to the following:**

Restrictions:

- **base:** xsd:string

Attribute Name: **ID**

Description: **File ID number**

Sample data: **37124**

Restrictions: **Data must adhere to the following:**

Description: **Must be a 5 digit number**

Restrictions:

- **base:** xsd:string
- **xsd:pattern:** [0-9]{5}
- **xsd:minLength:** 5
- **xsd:maxLength:** 5

This element contains the following other elements:

<Contents>

Description: **The ticket file may have only one "Contents" element which contains one or more ticket records**

Restrictions:

- **minOccurs:** 1 *** Required ***

- **maxOccurs: 1**

This element contains the following other elements:

<Ticket>

Description: **A Ticket Record**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: unbounded**

This element contains the following other elements:

<PrdHeader>

Description: **Ticket Header**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

This element contains the following other elements:

<TicketNumber>

Description: **Ticket number**
Sample data: 1A110001SS

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Ticket number**

- Restrictions:
- **type: TicketNumberType**

Description: **In order to prevent duplicate ticket numbers among the many TraCS agencies and locations across New York, the TraCS Universal Ticket Number is a unique 10-character value with the following components:**

- **Positions 1-4 are Machine code, alpha numeric only**
- **Machine code-This number MUST be UNIQUE within the issuing agency as it will become part of each Ticket and Accident Report number. The Criteria for the Machine Number is as follows:**
- **Position 1 cannot be zero or O**
- **Only letters and numbers are allowed, no special characters**

- All letters must be UPPER CASE
- The machine number MUST be exactly 4 characters long
- It can NOT start with Zero or the letter "O"
- The 4th character MUST be a number
- The first 3 characters of the machine number should not spell or imply anything offensive; the machine number is the first 4 characters of the Ticket number, and the third - sixth characters of the Accident Report number and as such will be seen by the public
- Position 4 must be numeric

Positions 5-8: TraCS Sequence Numbering- (Modified Base 30). A TraCS-generated sequence value using numbers and letters that allows for over 800,000 combinations:

- Created by using the letters of the alphabet A-Z plus 0-9 characters minus vowels (A,E,I,O,U,Y)
- Insures that the ticket will not spell or imply anything offensive
- Recommend in place of using only numerics so more than 9999 tickets can be written

Positions 9 and 10 are the agency code as assigned by DMV

Data must adhere to the following:

- Restrictions:
- base: xsd:string
 - xsd:minLength: 10
 - xsd:maxLength: 10

</TicketNumber>

<NCIC>

Description: National Crime Information Center Code
Sample data: 13102

Restrictions: • minOccurs: 1 *** Required ***
• maxOccurs: 1

Description: National Crime Information Center Code

Electronic Ticket/Accident Reporting Specifications

Restrictions:

Description: **The 5 position numeric National Crime Information Center Code for the enforcement agency that issued the traffic ticket. The number must match the NCIC as listed in Adjudication and must match the cross-referenced NCIC_TICKET_CDE in the last two positions of the ticket-number, as issued by DMV. (Note: The NCIC that is used is the middle 5 characters of the full 9 character value. For instance, NY1110100 would then be 11101. The NY and 00 are removed.)**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 5
 - **xsd:maxLength:** 5

</NCIC>

<BadgeNumber>

Description: **Officer ID**
Sample data: 9999

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer ID**

Restrictions:

Description: **The police badge number or officer Id is required and must already be on file with DMV for all Adjudication tickets. The badge number along with the NCIC is used to retrieve the Officer Name.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 5

</BadgeNumber>

<ArrestingOfficerInitials>

Description: **Officer initials**
Sample data: SO

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Electronic Ticket/Accident Reporting Specifications

Description: **Officer initials**

Restrictions:

Description: **The first 3 of the officers last name or the officer's initials. Useful in reporting back to the court and enforcement agency.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 3

</ArrestingOfficerInitials>

<ArrestingOfficerName>

Description: **Officer Name**

Sample data: **SAMPLE OFFICER**

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer Name**

Restrictions:

Description: **Used if the Officer initials are not present.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 20

</ArrestingOfficerName>

<OfficerSignature>

Description: **Officer signature**

Sample data: **R0IGODlh6wA3AMQAAAAAAP///wAAAAAAAAAAAA (Actual code representing signature is in excess of 12 lines; it has been abridged here to conserve page space.)
kuSV0uHj55U0ejmmmNGaeSV+aX67JZptqDRECADs=**

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer signature**

Restrictions:

Signature must be in encoded Base 64 .gif format

Description: **Long string**
Data must adhere to the following:
 Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 0

</OfficerSignature>

<TVB>

Description: **TVB: This element should left blank**
Sample data: N

Restrictions:

- **minOccurs:** 1 *** **Required** ***
- **maxOccurs:** 1

Description: **TVB**

Restrictions:

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string

Data table:

Value:	Literal:
Y	Ticket has been adjudicated
	Ticket has not been adjudicated

</TVB>

<Radar_Officer_Signature>

Description: **Radar officer signature - must appear for ticket involving radar. Otherwise can be omitted or left blank**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Radar officer signature**

Restrictions: **Signature must be in encoded Base 64 .gif format**

Description: **Not used by TSLED or adjudication**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 0

</Radar_Officer_Signature>
</PrdHeader>

<Motorist>

Description: **Motorist**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

This element contains the following other elements:

<FirstName>

Description: **Motorist's First Name**
Sample data: SALLY

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **First Name**

Restrictions:

Description: **Alpha characters and '-' (dash) are valid. The dash cannot be the first or last character. It is required for M or F gender code and Not required for gender of C for corporation.**

Data must adhere to the following:

Restrictions:

- **base: xsd:string**
- **xsd:minLength: 0**
- **xsd:maxLength: 20**

</FirstName>

<MI>

Description: **Motorist's Middle Initial, or Middle Name**
Sample data: D

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Middle Initial, or Middle Name**

Restrictions:

Description: **Must be alpha-only**

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

- **xsd:minLength:** 0
- **xsd:maxLength:** 20

</MI>

<LastName>

Description: **Motorist's Last Name**
Sample data: **SAMPLE**

Restrictions:

- **minOccurs:** 1 *** Required ***
- **maxOccurs:** 1

Description: **Last Name**

Restrictions:

Description: **Last Name can only contain alpha characters, '-' (dash), and '.' (periods). The dash cannot be the first or last position. The period can only be in the 3rd position following ST.**

Data must adhere to the following:

- Restrictions:
 - **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 20

</LastName>

<Suffix>

Description: **Motorist's Suffix**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Suffix Name: If supplied, must be one of the DMV acceptable suffixes**

Restrictions:

- **type:** NameSuffixType

Description: **Suffix**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
 - **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 5

Data table:

Value:	Literal:
---------------	-----------------

Electronic Ticket/Accident Reporting Specifications

II	II
III	III
IV	IV
JR	JR
SR	SR
2	2
2ND	2ND
3	3
3RD	3RD
4	4
4TH	4TH
5	5
5TH	5TH
6	6
6TH	6TH

</Suffix>

<StreetAddress>

Description: **Motorist's Residence Street Address**
Sample data: 1010 ANYPLACE ST

Restrictions:

- minOccurs: 1 *** Required ***
- maxOccurs: 1

Description: **Street Address**

Restrictions:

Description: **Alpha numeric or '&' or '/' or '%' or '-' or spaces are the only valid entries**

Data must adhere to the following:

Restrictions:

- base: xsd:string
- xsd:minLength: 0
- xsd:maxLength: 20

</StreetAddress>

<City>

Description: **Motorist’s Residence City**
Sample data: YOURCITY

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Residence City**

Restrictions:

Description: **Alpha or '-' or spaces are the only valid characters**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 20

</City>

<State>

Description: **Motorist’s Residence State**
Sample data: NY

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **State or province**

- Restrictions:
- **type:** StateType

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

- Description: **Select an option from the list**
- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA

Electronic Ticket/Accident Reporting Specifications

AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN

Electronic Ticket/Accident Reporting Specifications

MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND

Electronic Ticket/Accident Reporting Specifications

SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<ZipCode>

Description: **Motorist's Residence Zip-Code**

Sample data: 12121

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Zip-Code**

- Restrictions:
- **type:** FormatZipCodeType

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:pattern:** [0-9]{5}(-[0-9]{4})?
 - **xsd:minLength:** 5
 - **xsd:maxLength:** 10

</ZipCode>

<DateOfBirth>

Description: **Motorist's Birth Date: If the Gender is Male or Female, the date of birth (DOB) of the motorist is required**

Sample data: 7/18/1993

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Birth date**

- Restrictions:
- **type: DateTracsType**

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 8**
 - **xsd:maxLength: 10**

</DateOfBirth>

<Age>

Description: **Motorist's Age**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Age**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**

</Age>

<DateExpires>

Description: **License Expiration Date**
Sample data: 7/18/2013

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Electronic Ticket/Accident Reporting Specifications

Description: **License Expiration Date**

Restrictions:

- **type:** DateTracsType

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 8
- **xsd:maxLength:** 10

</DateExpires>

<Gender>

Description: **Motorist's Gender (Code)**
Sample data: F

Restrictions:

- **minOccurs:** 1 *** **Required** ***
- **maxOccurs:** 1

Description: **Gender**

Restrictions:

- **type:** GenderType

Description: **Gender**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
M	Male
F	Female
C	Corporation
U	Unknown

</Gender>

<License>

Electronic Ticket/Accident Reporting Specifications

Description: **License. Required if there is a license present.**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Driver's license**

- Restrictions:
- **type:** MotoristLicenseType

Description: **Motorist License**

This element contains the following other elements:

<Number>

Description: **Drivers License Number**

- Restrictions:
- **minOccurs:** 1 ***** Required *****
 - **maxOccurs:** 1

Description: **Out Of State License Number or NY Client Id**
Sample data: 00000000

Restrictions:

Description: **If the accused is not a corporation, and the motorist is licensed in a state other than NY, this would be the motorist's license number from the issuing state. If unlicensed, this field should be left blank. Format: Alphanumeric Only, 25 character maximum. If the accused is not a corporation, and the motorist's license is from NY this should be the NYS Client-Id from their license. This is always a nine-numeric, never (00000000) or (55555555) or (99999999). 9 character maximum length. If unknown or unlicensed, this field should be left blank.**

Data must adhere to the following:

Description: **A minimum length of zero allows the element to be left blank.**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 25

</Number>

<State>

Description: **State license issued in. Required if there is a license present**
Sample data: NY

Electronic Ticket/Accident Reporting Specifications

Restrictions: • **minOccurs: 1 *** Required *****

• **maxOccurs: 1**

Description: **State or province**

Restrictions: • **type: StateType**

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM

Electronic Ticket/Accident Reporting Specifications

HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA

Electronic Ticket/Accident Reporting Specifications

NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN

WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<Class>

Description: **License Class**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **License Class: If the accused is a licensed motorist from another state, then the Class of the motorist's license is required. If the motorist is not licensed or the class of the motorist's license cannot be determined, the default should be "UNK"**

Sample data: B

- Restrictions:
- **type:** LicenseClassType

Description: **Conditional - If the accused is a licensed motorist from another state, then the Class of the motorist's license is required. If the motorist is not licensed or the class of the motorist's license cannot be determined, the default should be "UNK".**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 3

Data table:

Value:	Literal:
A	Commercial, Class A: Commercial, Class A, Class B and Class C (CDL): Drivers age 21

Electronic Ticket/Accident Reporting Specifications

	<p>or over can apply for a Class A driver license or any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR) of 26,001 lbs. or more.</p>
B	<p>Commercial, Class B: Commercial, Class A, Class B and Class C (CDL): Drivers age 21 or over can apply for a Class A driver license or any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR) of 26,001 lbs. or more.</p>
C	<p>Commercial, Class C: Commercial, Class A, Class B and Class C (CDL): Drivers age 21 or over can apply for a Class A driver license or</p>

Electronic Ticket/Accident Reporting Specifications

	any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR) of 26,001 lbs. or more.
D	Operator, Class D: Issued to drivers age 18 or over, or to drivers age 17 with Driver Education. Valid for passenger cars and trucks with a gross vehicle weight rating (GVWR) of 26,000 lbs. or less. A Class D driver can drive a vehicle that tows another vehicle (for example a trailer) that has a maximum gross weight of 10,000 lbs. or less. A Class D driver can tow a vehicle with a GVWR of more than 10,000 lbs only if the combined weight rating of the two vehicles is 26,000 lbs. or less.
E	Taxi and Livery, Class E: Issued to drivers age 18 or over. Valid for the same vehicles that a

Electronic Ticket/Accident Reporting Specifications

	class D driver can drive, plus for-hire vehicles that carry 14 passengers or less.
DJ	Junior License, Class DJ: Issued to drivers under the age of 18, with restrictions. Read the DMV brochure, Learner Permits and Junior Licenses. Valid for passenger cars and trucks with a gross vehicle weight rating (GVWR) of 10,000 lbs. or less. A class DJ driver can drive a vehicle that tows another vehicle (for example a trailer) with a GVWR of 3,000 lbs. or less.
M	Motorcycle, Class M: for motorcycles.
MJ	Junior Motorcycle License, Class MJ: for motorcycle drivers under the age of 18, with restrictions.
NC	Non-CDL Class C: Changes for Class D drivers resulted from a law that eliminates the Non-CDL Class C license.
UNK	Unknown: If the motorist is not licensed or the class of the

	motorist's license cannot be determined.
--	--

Data must adhere to the following:

- Description: **For out-of-state licenses, enter the class from the license up to a maximum of three characters**
- Restrictions: **• base: xsd:string**
• xsd:maxLength: 3

</Class>

</License>

</Motorist>

<Vehicle>

- Description: **Vehicle**
- Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1
- Description: **Vehicle information**

This element contains the following other elements:

<PlateNumber>

- Description: **Plate Number**
Sample data: 123ABC
- Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1
- Description: **Plate Number**
- Restrictions:
- Description: **Alphanumeric plate number with no embedded spaces or special characters.**
- Data must adhere to the following:**
- Restrictions: **• base: xsd:string**
• xsd:minLength: 1
• xsd:maxLength: 8

</PlateNumber>

<PlateState>

Description: **Registration State**
Sample data: NY

Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1

Description: **State vehicle is registered in**

Restrictions: **• type: StateType**

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions: **• base: xsd:string**
• xsd:minLength: 2
• xsd:maxLength: 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE

Electronic Ticket/Accident Reporting Specifications

GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE

Electronic Ticket/Accident Reporting Specifications

NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT

WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</PlateState>

<VehicleType>

Description: **Vehicle Type: Type of vehicle the defendant was driving or occupying at the time of the offense. Used to validate certain violations. Default: 1 Passenger**
Sample data: 1

Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1

Description: **Vehicle TypeDefault: 1 Passenger**

Restrictions: **• type: VehicleTypeType**

Description: **Type of vehicle**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions: **• base: xsd:string**
• xsd:minLength: 1
• xsd:maxLength: 1

Data table:

Value:	Literal:
0	No vehicle
1	Passenger
2	Bus
3	Motorcycle
4	Moped
5	Truck
6	Truck/Tractor

Electronic Ticket/Accident Reporting Specifications

7	Recreation vehicle
8	Farm vehicle
9	All others
A	All terrain vehicle
B	Bicycle
P	Pick up truck
V	Van

</VehicleType>

<Make>

Description: **Vehicle Make**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Vehicle Make**

Restrictions:

- **type:** VehicleMakeType

Description: **Maximum of 5 character Vehicle Make**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 5

Data table:

Value:	Literal:
-3	Not Entered
-2	Not Applicable
-1	Unknown Make
1	American Motors*
2	Jeep* (Includes Willys/Kaiser-Jeep)
3	AM General
4	Chrysler/DaimlerChrysler
5	Dodge

Electronic Ticket/Accident Reporting Specifications

6	Imperial
7	Plymouth
8	Eagle*
9	Ford
10	Lincoln
11	Mercury
12	Buick
13	Cadillac
14	Chevrolet
15	Oldsmobile
16	Pontiac
17	GMC
18	Saturn
19	Grumman/Grumman-Olson
20	Other Domestic Manufacturers
21	Volkswagen
22	Alfa Romeo
23	Audi
24	Austin/Austin Healey
25	BMW
26	Nissan/Datsun
27	Fiat
28	Honda
29	Isuzu
30	Jaguar
31	Lancia
32	Mazda
33	Mercedes-Benz

Electronic Ticket/Accident Reporting Specifications

34	MG
35	Peugeot
36	Porsche
37	Renault
38	Saab
39	Subaru
40	Toyota
41	Triumph
42	Volvo
43	Mitsubishi
44	Suzuki
45	Acura
46	Hyundai
47	Merkur
48	Yugo
49	Infiniti
50	Lexus
51	Daihatsu
52	Sterling
53	Land Rover
54	KIA
55	Daewoo
56	Other Import
57	BSA
58	Ducati
59	Harley-Davidson
60	Kawasaki
61	Moto-Guzzi

Electronic Ticket/Accident Reporting Specifications

62	Norton
63	Yamaha
64	Brockway
65	Diamond Reo or Reo
66	Freightliner
67	FWD
68	International Harvester/Navistar
69	Kenworth
70	Mack
71	Peterbilt
72	Iveco/Magirus*
73	White/Autocar-WhiteGMC
74	Bluebird
75	Eagle Coach
76	Gillig
77	MCI
78	Thomas Built
79	Other Make *

</Make>

<Year>

Description: **Vehicle Year**
Sample data: 1997

Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1

Description: **Vehicle Year**

Restrictions:

Data must adhere to the following:

Restrictions: **• base: xsd:string**
• xsd:minLength: 4

- **xsd:maxLength: 4**

</Year>

<RegExpires>

Description: **Registration Expiration**
Sample data: 6/30/2006

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Registration Expiration Date**

Restrictions: • **type: DateTracsType**
Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 8**
 - **xsd:maxLength: 10**

</RegExpires>

<VehColor>

Description: **Vehicle Color**
Sample data: BK

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Vehicle Color**

Restrictions: • **type: VehicleColorType**

Data must adhere to the following:

Description: **When vehicle information is returned in a batch registration inquiry, the color of the vehicle will be represented by the elements DMV_VEH_COLOR1_CDE and DMV_VEH_COLOR2_CDE.**

The following table lists the codes that may be returned to indicate the color of a registered vehicle:

Color Codes

Electronic Ticket/Accident Reporting Specifications

Standard Color Codes : (may be returned as Color1 or Color2)

BK: Black	OR: Orange
BL: Blue	PK: Pink
BR: Brown	PR: Purple
GL: Gold	RD: Red
GR: Green	TN: Tan
GY: Gray	WH: White
MR: Maroon	YW: Yellow

Special Color Codes : (see “Color Combinations” for more information)

DK Dark	- Used to modify a standard color. Can be returned only as Color1
LT Light	- Used to modify a standard color. Can be returned only as Color1
NO No	- Can be returned only as Color1, and only if paired with “CL”
CL Color	- Can be returned only as Color2, and only if paired with “NO”.

Color Combinations

If both Color1 and Color2 are returned, it will be necessary to examine both codes to determine the meaning:

- **If both Color1 and Color2 are “standard colors” as listed in the table above, then it means that the vehicle is painted in those two colors.**
- **If Color1 is “DK” or “LT”, then the vehicle is painted a dark or light shade of the color indicated in Color2.**

- If Color1 is “NO” and Color2 is “CL”, it means that the DMV file does not have any color information for the vehicle (i.e., the color of the vehicle is unknown).

Here are some example combinations:

Color1	Color2	Interpretation
RD	BK	Red and Black
DK	GY	Dark Gray
LT	GR	Light Green
NO	CL	No color (color unknown)

Restrictions: • **base:** xsd:string

</VehColor>

<VIN>

Description: **Vehicle Identification Number**

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **Vehicle Identification Number**

Restrictions:

Data must adhere to the following:

Restrictions: • **base:** xsd:string

</VIN>

<RegisteredWeight>

Description: **Registered vehicle Weight**

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Registered vehicle Weight**

Restrictions:

Description: **Required for weight violations. See Conditional Table.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 6

</RegisteredWeight>

<ActualWeight>

Description: **Actual vehicle Weight**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Actual vehicle Weight**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 6

</ActualWeight>

<NumberOfAxles>

Description: **Number of Axles**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Number of Axles**

Restrictions:

Description: **Required for certain Registration Violations. See Conditional Table.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 2

</NumberOfAxles>

<Commercial>

Description: **Commercial vehicle indicator**

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Commercial vehicle indicator**

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **type:** CommercialVehicleIndicatorType
- Description: **Values "C" If the Vehicle is Commercial, otherwise Blank.**
- Data must adhere to the following:**
- Description: **Select an option from the list**
- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
C	Commercial Vehicle
	Non commercial vehicle

</Commercial>

<Bus>

- Description: **Bus Indicator**
- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1
- Description: **Bus Indicator**
- Restrictions:
- **type:** BusIndicatorType
- Description: **Values "B" If the Vehicle is a Commercial Bus, otherwise Blank.**
- Data must adhere to the following:**
- Description: **Select an option from the list**
- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
B	Bus
	Not a bus

</Bus>

<HazardousMaterial>

- Description: **HazMat Indicator**

Electronic Ticket/Accident Reporting Specifications

Restrictions:

- **minOccurs:** 1 *** **Required** ***
- **maxOccurs:** 1

Description: **HazMat Indicator**

Restrictions:

- **type:** HazardousMaterialIndicatorType

Description: **Values: "H" If the Vehicle is carrying Hazardous Materials or Placarded as such, otherwise Blank.**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
H	Haz Mat
	Non HazMat vehicle

</HazardousMaterial>

<OwnerOwned>

Description: **Owner owned**
Sample data: 1

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Owner owned**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:maxLength:** 1

</OwnerOwned>

<DOTNumber>

Description: **US Dot Number**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Electronic Ticket/Accident Reporting Specifications

Description: **US Dot Number**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 8

</DOTNumber>

</Vehicle>

<Court>

Description: **Court**

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

This element contains the following other elements:

<Code>

Description: **DCJS Court Code - ORI Number: Court code that the ticket is answerable to**
Sample data: NY031121J

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1
 - **type:** FormatStringORI

Description: **ORI #**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:pattern:** [N][Y][0-9]{6}[J]
 - **xsd:minLength:** 9
 - **xsd:maxLength:** 9

</Code>

<Name>

Description: **Court name**
Sample data: YOUR TOWN COURT

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Court name**

Restrictions:

Data must adhere to the following:

Restrictions: • **base:** xsd:string

</Name>

<StreetAddress>

Description: **Court Street Address**

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **Street Address**

Restrictions:

Description: **Alpha numeric or '&' or '/' or '%' or '-' or spaces are the only valid entries**

Data must adhere to the following:

Restrictions: • **base:** xsd:string
 • **xsd:minLength:** 0
 • **xsd:maxLength:** 20

</StreetAddress>

<City>

Description: **Court City**
 Sample data: COURT CITY

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **Residence City**

Restrictions:

Description: **Alpha or '-' or spaces are the only valid characters**

Data must adhere to the following:

Restrictions: • **base:** xsd:string
 • **xsd:minLength:** 0
 • **xsd:maxLength:** 20

</City>

<State>

Description: **Court State: Must be set to NY**
 Sample data: NY

Electronic Ticket/Accident Reporting Specifications

Restrictions: • **minOccurs: 1 *** Required *****

• **maxOccurs: 1**

Description: **State or province**

Restrictions: • **type: StateType**

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII

Electronic Ticket/Accident Reporting Specifications

IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA

Electronic Ticket/Accident Reporting Specifications

NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING

Electronic Ticket/Accident Reporting Specifications

YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<ZipCode>

Description: **Court Zip Code**
Sample data: 12345

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Zip-Code**

Restrictions:

- **type: FormatZipCodeType**
Data must adhere to the following:
Restrictions:
 - **base: xsd:string**
 - **xsd:pattern: [0-9]{5}(-[0-9]{4})?**
 - **xsd:minLength: 5**
 - **xsd:maxLength: 10**

</ZipCode>

<CourtDate>

Description: **Appearance Date: The date, by which, the motorist is ordered to answer the charge on the ticket. If this date is in an incorrect format, missing, more than a year in the future or prior to the violation date an Exception will be generated**
Sample data: 12/27/2005

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Appearance Date: The date, by which, the motorist is ordered to answer the charge on the ticket. If this date is in an incorrect format, missing, more than a year in the future or prior to the violation date an Exception will be generated**

Restrictions:

- **type: DateTracsType**
Description: **Date**
Data must adhere to the following:
Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**
Restrictions:
 - **base: xsd:string**

- **xsd:minLength:** 8
- **xsd:maxLength:** 10

</CourtDate>

<CourtTime>

Description: **Appearance Time: The time at which the motorist is ordered to answer the charge on the ticket**
Sample data: 19:00

Restrictions:

- **minOccurs:** 1 *** Required ***
- **maxOccurs:** 1

Description: **Appearance Time**

Restrictions:

Data must adhere to the following:

Description: **Must match the pattern: HH:MM using the 24 hour clock**

Restrictions:

- **base:** xsd:string
- **xsd:pattern:** [0-2]{1}[0-9]{1};[0-5]{1}[0-9]{1}
- **xsd:minLength:** 5
- **xsd:maxLength:** 5

</CourtTime>

<DWITest>

Description: **DWI Test. Alcohol and Drug tests and results data is required in the violation section**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **DWI Test**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string

</DWITest>

<TestType>

Description: **Test type: Alcohol and Drug tests and results data is required in the violation section**

Restrictions:

- **minOccurs:** 0

- **maxOccurs: 1**

Description: **Test type**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</TestType>

<TestResults>

Description: **Test results: Alcohol and Drug tests and results data is required in the violation section**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Test results**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</TestResults>

<OfficerNotes>

Description: **Officer Notes**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Officer Notes This element is not currently used.**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</OfficerNotes>

<ReturnByMail>

Description: **Return By Mail**
Sample data: 1

Restrictions:

- **minOccurs: 1 *** Required *****

- **maxOccurs: 1**

Description: **Return By Mail**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**

</ReturnByMail>

</Court>

<SupportingDeposition>

Description: **Supporting Deposition**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

This element contains the following other elements:

<Type>

Description: **Type of deposition**
Sample data: 1

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Type of supporting deposition**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**

</Type>

<Information>

Description: **Information**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Information on supporting deposition**

Restrictions:

Description: **Used for exceptions**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 500

</Information>

<DefendantStatement>

Description: **Type of deposition**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Type of deposition**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</DefendantStatement>

<ChargeBased>

Description: **Charge Based**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Charge Based**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</ChargeBased>

<DirectionTravel>

Description: **Direction of Travel**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Direction of Travel**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</DirectionTravel>

</SupportingDeposition>

<Violation>

Description: **Violation**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

This element contains the following other elements:

<ViolationDate>

Description: **Date and time of violation**
Sample data: 12/18/200508:01:00

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Date and time of violation**

- Restrictions:
- **type: DateTimeTracsType**

Description: **Date and time of the occurrence of the violation. Format: MM/DD/YYYYHH:MM:SS OR MM/DD/YYYY HH:MM:SS The Violation date cannot be in the future and cannot be more than 2 years old.**

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 13**
 - **xsd:maxLength: 22**

</ViolationDate>

<TypeOfLaw>

Description: **Law Type: The type of law the section the violation charged is based on, as printed on the motorists' copy of the ticket (should match the first 3 characters of the DCJSCode)**
Sample data: VTL

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Law Type**

- Restrictions:
- **type: TypeOfLawType**

Description: **The type of law**

Data must adhere to the following:

- Description: **Select an option from the list**

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 3

Data table:

Value:	Literal:
PL	Penal Law
TAX	Tax Law
TL	Transportation Law
VTL	Vehicle/Traffic Law

</TypeOfLaw>

<ViolationCharged>

Description: **DCJS Law Code: DCJS Encoded Violation Code for Violation Charged**
Sample data: VTL0375 31 0I0

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **DCJS Law Code**

Restrictions:

Description: **DCJS Encoded Violation Code for Violation Charged**
(see Violation Codes table)

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 22

</ViolationCharged>

<ActualSpeed>

Description: **Actual Speed Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater than 5 and less than 200. Must be greater than speed zone.**
Sample data: 000

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Actual Speed**

Electronic Ticket/Accident Reporting Specifications

Restrictions:

Description: **Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater than 5 and less than 200. Must be greater than speed zone.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:integer
 - **xsd:minExclusive:** 5
 - **xsd:maxExclusive:** 200

</ActualSpeed>

<ZoneSpeed>

Description: **Zone Speed - Posted Limit: Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater or equal to 5 and less than or equal to 65 in multiples of 5. Must be less than actual speed. Sample data: 000**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Zone Speed - Posted Limit**

Restrictions:

Description: **Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater or equal to 5 and less than or equal to 65 in multiples of 5. Must be less than actual speed.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:integer
 - **xsd:minInclusive:** 5
 - **xsd:maxInclusive:** 65

</ZoneSpeed>

<HighwayTypeCode>

Description: **Highway Type: Type of road the violation occurred on Sample data: 3**

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Highway Type: Type of road the violation occurred on**

- Restrictions:
- **type:** HighwayTypeCodeType

Description: **Type of road**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Interstate
2	State highway
3	County
4	Town
5	Village
6	City
7	Off road
8	Parking lot
9	Parkway

</HighwayTypeCode>

<RouteCode>

Description: **Route Code**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Route Code**

Restrictions:

Description: **If the Highway type is 1(Interstate), 2(State highway) or 9(Parkway) the route code is required, otherwise it is optional. - Type 9 is per TSLED Lookup (parkway)**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 4

Data table:

Electronic Ticket/Accident Reporting Specifications

Value:	Literal:
BDPK	Bay Drive
BRPK	Bronx River Parkway
BSPK	Bethpage State Parkway
CCPK	Cross County Parkway
HRPK	Hutchinson River Parkway
HSPK	Heckscher Spur
LMPK	Long Mountain Parkway
LOPK	Lake Ontario State Parkway
LPKY	Loop Parkway
MCPK	Robert Moses Causeway
MSPK	Meadowbrook Parkway
NSPK	Northern State Parkway
OCPK	Ocean Parkway
PIPK	Palisades Interstate Parkway
RMPK	Robert Moses Parkway
SAPK	Sagtikos State Parkway
SBPK	Sprain Brook Parkway
SMPK	Saw Mill River Parkway
SOPK	South State Parkway
SSPK	Southern State Parkway
SUPK	Sunken Meadow Spur
TSPK	Taconic State Parkway
UNKN	Unknown
WRPK	W. River St Parkway
WSPK	Wantagh State Parkway

</RouteCode>

<MuniCode>

Electronic Ticket/Accident Reporting Specifications

Description: **Muni Code: 4-digit municipality code where the violation occurred. Should agree with the municipalities the NCIC can write tickets to and the municipalities answerable to the court**
Sample data: 3452

Restrictions:

- minOccurs: 1 *** Required ***
- maxOccurs: 1

Description: **Muni Code**

Restrictions:

Description: **4-digit municipality code where the violation occurred. Should agree with the municipalities the NCIC can write tickets to and the municipalities answerable to the court - per TSLED Lookups.**

Data must adhere to the following:

Restrictions:

- base: xsd:string
- xsd:minLength: 4
- xsd:maxLength: 4

</MuniCode>

<Municipality>

Description: **Municipality**
Sample data: TOWN OF CLAY

Restrictions:

- minOccurs: 0
- maxOccurs: 1

Description: **Municipality**

Restrictions:

Data must adhere to the following:

Restrictions:

- base: xsd:string

</Municipality>

<ArrestTypeCode>

Description: **Arrest Type**
Sample data: 1

Restrictions:

- minOccurs: 1 *** Required ***
- maxOccurs: 1

Description: **Arrest Type**

Restrictions:

Electronic Ticket/Accident Reporting Specifications

Description: **Per TSLED Lookup - Arrest Type Will default to the code for “Unknown” if the data is not present or not on database Arrest_Type table. This field serves as the indicator as to whether the charge is based on a property, personal injury or fatal accident.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Patrol
2	Radar
3	Road check
4	Scales
5	Property damage accident
6	Personal injury accident
7	Fatal accident
8	Aircraft
9	Other
L	Laser
V	Vascar
W	Work zone

</ArrestTypeCode>

<AlcoholDrugTest>

Description: **Alcohol-Drug test Administered Code**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Alcohol-Drug test Administered Code**

- Restrictions:
- **type:** AlcoholDrugTestAdministeredType

Description: **If 1192.X (Drug or alcohol related offense) a code indicating whether a test for alcohol or drugs was given**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Test given, results required
2	Test refused
3	No test given
4	Unknown if test was given

</AlcoholDrugTest>

<AlcoholDrugTestType>

Description: **Alcohol-Drug Test Type Code**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Alcohol-Drug Test Type Code**

- Restrictions:
- **type:** AlcoholDrugTestTypeType

Description: **If 1192.X, and a test for alcohol or drugs was administered, a code of the type of test**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Breathalyzer
2	Blood test
3	Urinalysis

</AlcoholDrugTestType>

<AlcoholTestResult>

Description: **Alcohol Test Result: If 1192.1,2,3,5,6 and a test for alcohol was administered, a two-digit number between 00 and 60, when multiplied by .10 is equal to the BAC of the test result.**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Alcohol Test Result**

Restrictions:

Description: **If 1192.1,2,3,5,6 and a test for alcohol was administered, a two-digit number between 00 and 60, when multiplied by .10 is equal to the BAC of the test result.**

Data must adhere to the following:

Description: **A two-digit number between 00 and 60**

Restrictions:

- **base:** xsd:string
- **xsd:pattern:** [0-6]{1}[0-9]{1}
- **xsd:minLength:** 2
- **xsd:maxLength:** 2

</AlcoholTestResult>

<DrugTestResult>

Description: **Drug Test Result**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Drug Test Result**

Restrictions:

- **type:** DrugTestResultType

Description: **If 1192.4 and a test for drugs was administered**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
---------------	-----------------

Electronic Ticket/Accident Reporting Specifications

P	Positive
N	Negative

</DrugTestResult>

<ArrestTransactionDate>

Description: **Arrest Transaction Date**
Sample data: 12/18/200500:00:00

- Restrictions:
- minOccurs: 0
 - maxOccurs: 1

Description: **Arrest Transaction Date**

Restrictions: • type: DateTimeTracsType

Description: **Date and time of the occurrence of the violation. Format: MM/DD/YYYYHH:MM:SS OR MM/DD/YYYY HH:MM:SS The Violation date cannot be in the future and cannot be more than 2 years old.**

Data must adhere to the following:

- Restrictions:
- base: xsd:string
 - xsd:minLength: 13
 - xsd:maxLength: 22

</ArrestTransactionDate>

<LocalOffice>

Description: **Local Office - TZS: For State Police, this field is the Troop/Zone/Sector(TZS). For others, this can be a precinct or sub station.**
Sample data: A111

- Restrictions:
- minOccurs: 1 *** Required ***
 - maxOccurs: 1

Description: **Local Office - TZS**

Restrictions:

Description: **For State Police, this field is the Troop/Zone/Sector(TZS). For others, this can be a precinct or sub station.**

Data must adhere to the following:

- Restrictions:
- base: xsd:string
 - xsd:minLength: 1
 - xsd:maxLength: 4

</LocalOffice>

<PoliceAgency>

Description: **NCIC Description: Used for exceptions**
Sample data: TOWN OF CLAY POLICE

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **NCIC Description**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**
- **xsd:minLength: 1**
- **xsd:maxLength: 30**

</PoliceAgency>

<CTVName>

Description: **CTV Name**
Sample data: 3452

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **CTV Name**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</CTVName>

<PlaceOfOccurance>

Description: **Place Of Occurance**
Sample data: SOULE ROAD

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Place Of Occurance**

Restrictions:

Data must adhere to the following:

Electronic Ticket/Accident Reporting Specifications

Restrictions: • **base:** xsd:string
</PlaceOfOccurance>

<DriverLicShown>

Description: **Driver's License Shown**
Sample data: **1**

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **Driver's License Shown**

Restrictions:

Data must adhere to the following:

 Restrictions: • **base:** xsd:string

</DriverLicShown>

<ViolationDescription>

Description: **Violation Description**
Sample data: **INADEQUATE MUFFLER-LOUD**

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **Violation Description**

Restrictions:

Data must adhere to the following:

 Restrictions: • **base:** xsd:string

</ViolationDescription>

<LawSection>

Description: **VT Code: Violation Charged - Must match DMV violation code table.**
Sample data: **37531**

Restrictions: • **minOccurs:** 1 *** **Required** ***
 • **maxOccurs:** 1

Description: **VT Code**

Restrictions:

Description: **Violation Charged - Must match DMV violation code table.**

Data must adhere to the following:

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 7

</LawSection>

<Ordinal>

Description: **Ordinal**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Ordinal**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</Ordinal>

</Violation>

<Location>

Description: **Location: Not used by TSLED**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

</Location>

</Ticket>

</Contents>

</File

Sample Adjudication XML File

```

<File name="Abc_file" ID="37124">
  <Contents>
    <Ticket>
      <PrdHeader>
        <TicketNumber>
          1A110001SS
        </TicketNumber>
        <NCIC>
          13102
        </NCIC>
        <BadgeNumber>
          9999
        </BadgeNumber>
        <ArrestingOfficerInitials>
          SO
        </ArrestingOfficerInitials>
        <ArrestingOfficerName>
          SAMPLE OFFICER
        </ArrestingOfficerName>
        <OfficerSignature>
          R0IGODlh6wA3AMQAAAAAP///wAAAAAAAAAAAA
          (Actual code representing signature is in excess of 12 lines;
          it has been abridged here to conserve page space.)
          kuSVOuHj55U0ejmnmNGaeSV+aX67JZptqDRECADs=
        </OfficerSignature>
        <TVB>
          Y
        </TVB>
        <Radar_Officer_Signature>
        </Radar_Officer_Signature>
      </PrdHeader>
    <Motorist>
      <FirstName>
        SALLY
      </FirstName>
      <MI>
        D
      </MI>
      <LastName>
        SAMPLE
      </LastName>
      <Suffix>
      </Suffix>
      <StreetAddress>
        1010 ANYPLACE ST
      </StreetAddress>

```

```
<City>
YOURCITY
</City>
<State>
NY
</State>
<ZipCode>
12121
</ZipCode>
<DateOfBirth>
7/18/1993
</DateOfBirth>
<DateExpires>
7/18/2013
</DateExpires>
<Gender>
F
</Gender>
<License>
  <Number>
  </Number>
  <State>
  NY
  </State>
  <Class>
  </Class>
</License>
</Motorist>
<Vehicle>
  <PlateNumber>
  123ABC
  </PlateNumber>
  <PlateState>
  NY
  </PlateState>
  <RegistrationType>
  </RegistrationType>
  <VehicleType>
  1
  </VehicleType>
  <Make>
  </Make>
  <Year>
  1997
  </Year>
  <RegExpires>
  6/30/2006
  </RegExpires>
```

```
<VehColor>
BK
</VehColor>
<RegisteredWeight>
</RegisteredWeight>
<NumberOfAxles>
</NumberOfAxles>
<Commercial>
</Commercial>
<Bus>
</Bus>
<HazardousMaterial>
</HazardousMaterial>
<OwnerOwned>
1
</OwnerOwned>
<DOTNumber>
</DOTNumber>
</Vehicle>
<Court>
<Code>
NY031121J
</Code>
<StreetAddress>
</StreetAddress>
<City>
</City>
<State>
</State>
<ZipCode>
</ZipCode>
<CourtDate>
</CourtDate>
<CourtTime>
</CourtTime>
<DWITest>
</DWITest>
<TestType>
</TestType>
<TestResults>
</TestResults>
<OfficerNotes>
</OfficerNotes>
<ReturnByMail>
</ReturnByMail>
</Court>
<SupportingDeposition>
<Type>
```

```
</Type>
<Information>
</Information>
<DefendantStatement>
</DefendantStatement>
<ChargeBased>
</ChargeBased>
<DirectionTravel>
</DirectionTravel>
</SupportingDeposition>
<Violation>
  <ViolationDate>
    12/18/200508:01:00
  </ViolationDate>
  <TypeOfLaw>
    VTL
  </TypeOfLaw>
  <DCJSCode>
    VTL0375 31 010
  </DCJSCode>
  <ActualSpeed>
  </ActualSpeed>
  <ZoneSpeed>
  </ZoneSpeed>
  <HighwayTypeCode>
  </HighwayTypeCode>
  <RouteCode>
  </RouteCode>
  <MuniCode>
  </MuniCode>
  <ArrestTypeCode>
  </ArrestTypeCode>
  <ArrestTransactionDate>
  </ArrestTransactionDate>
  <LocalOffice>
    A111
  </LocalOffice>
  <PoliceAgency>
  </PoliceAgency>
  <CTVName>
  </CTVName>
  <PlaceOfOccurance>
  </PlaceOfOccurance>
  <DriverLicShown>
  </DriverLicShown>
  <ViolationDescription>
  </ViolationDescription>
  <LawSection>
```

```
3752A1
</LawSection>
<Ordinal>
06600
</Ordinal>
<AlcoholDrugTest>
</AlcoholDrugTest>
<AlcoholDrugTestType>
</AlcoholDrugTestType>
<AlcoholTestResult>
</AlcoholTestResult>
<DrugTestResult>
</DrugTestResult>
</Violation>
<Location>
</Location>
</Ticket>
</Contents>
</File>
```

Adjudication Data Elements

Description: Adjudication Ticket Data Elements: The following schema gives the requirements and descriptions for each data element as it is used and viewed by Adjudication

Additional information may be found on the TraCS Data Element RSS feed:

http://www.nycourts.gov/ea/XML/XML_Data/RSS/Tracs_Schema_RSS_20_Feed.xml

<File name="" ID="">

Description: **Ticket File**

Restrictions:

Attributes for: <File> Element (NYSP creates the file element (Name and ID.) Do not include this element in your files.)

Attribute Name: **name**

Description: **File name**

Sample data: Abc_file

Restrictions: **Data must adhere to the following:**

Restrictions: **• base: xsd:string**

Attribute Name: **ID**

Description: **File ID number**

Sample data: 37124

Restrictions: **Data must adhere to the following:**

Description: **Must be a 5 digit number**

- Restrictions:
- base: xsd:string**
 - xsd:pattern: [0-9]{5}**
 - xsd:minLength: 5**
 - xsd:maxLength: 5**

This element contains the following other elements:

<Contents>

Description: **The ticket file may have only one "Contents" element which contains one or more ticket records**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

This element contains the following other elements:

<Ticket>

Description: **A Ticket Record**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: unbounded**

This element contains the following other elements:

<PrdHeader>

Description: **Ticket Header**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

This element contains the following other elements:

<TicketNumber>

Description: **Ticket number**
Sample data: 1A110001SS

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Ticket number**

- Restrictions:
- **type: TicketNumberType**

Description: **In order to prevent duplicate ticket numbers among the many TraCS agencies and locations across New York, the TraCS Universal Ticket Number is a unique 10-character value with the following components:**

- **Positions 1-4 are Machine code, alpha numeric only**

- **Machine code-This number MUST be UNIQUE within the issuing agency as it will become part of each Ticket and Accident Report number. The Criteria for the Machine Number is as follows:**
- **Position 1 cannot be zero or O**
- **Only letters and numbers are allowed, no special characters**

- All letters must be UPPER CASE
- The machine number MUST be exactly 4 characters long
- It can NOT start with Zero or the letter "O"
- The 4th character MUST be a number

- The first 3 characters of the machine number should not spell or imply anything offensive; the machine number is the first 4 characters of the Ticket number, and the third - sixth characters of the Accident Report number and as such will be seen by the public

- Position 4 must be numeric

Positions 5-8: TraCS Sequence Numbering- (Modified Base 30). A TraCS-generated sequence value using numbers and letters that allows for over 800,000 combinations:

- Created by using the letters of the alphabet A-Z plus 0-9 characters minus vowels (A,E,I,O,U,Y)
- Insures that the ticket will not spell or imply anything offensive
- Recommend in place of using only numerics so more than 9999 tickets can be written

Positions 9 and 10 are the agency code as assigned by DMV

Data must adhere to the following:

- Restrictions:
- base: xsd:string
 - xsd:minLength: 10
 - xsd:maxLength: 10

</TicketNumber>

<NCIC>

Description: National Crime Information Center Code
Sample data: 13102

Restrictions: • minOccurs: 1 *** Required ***
• maxOccurs: 1

Description: National Crime Information Center Code

Electronic Ticket/Accident Reporting Specifications

Restrictions:

Description: **The 5 position numeric National Crime Information Center Code for the enforcement agency that issued the traffic ticket. The number must match the NCIC as listed in Adjudication and must match the cross-referenced NCIC_TICKET_CDE in the last two positions of the ticket-number, as issued by DMV. . (Note: The NCIC that is used is the middle 5 characters of the full 9 character value. For instance, NY1110100 would then be 11101. The NY and 00 are removed.)**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 5
 - **xsd:maxLength:** 5

</NCIC>

<BadgeNumber>

Description: **Officer ID**
Sample data: 9999

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer ID**

Restrictions:

Description: **The police badge number or officer Id is required and must already be on file with DMV for all Adjudication tickets. The badge number along with the NCIC is used to retrieve the Officer Name.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 5

</BadgeNumber>

<ArrestingOfficerInitials>

Description: **Officer initials**
Sample data: SO

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer initials**

Electronic Ticket/Accident Reporting Specifications

Restrictions:

Description: **The first 3 of the officers last name or the officer's initials. Useful in reporting back to the court and enforcement agency.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 3

</ArrestingOfficerInitials>

<ArrestingOfficerName>

Description: **Officer Name**
Sample data: SAMPLE OFFICER

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer Name**

Restrictions:

Description: **Used if the Officer initials are not present.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 20

</ArrestingOfficerName>

<OfficerSignature>

Description: **Officer signature**
Sample data: R0IGODlh6wA3AMQAAAAAAP//wAAAAAAAAAAAA (Actual code representing signature is in excess of 12 lines; it has been abridged here to conserve page space.)
kuSVOuHj55U0ejmmnNGaeSV+aX67JZptqDRECADs=

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Officer signature**

Restrictions: **Signature must be in encoded Base 64 .gif format**

Description: **Long string**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0

</OfficerSignature>

<TVB>

Description: **TVB: This element should always be set to "Y" for adjudicated tickets**
Sample data: Y

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **TVB**

Restrictions:

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string

Data table:

Value:	Literal:
Y	Ticket has been adjudicated
	Ticket has not been adjudicated

</TVB>

<Radar_Officer_Signature>

Description: **Radar officer signature - must appear for ticket involving radar. Otherwise can be omitted or left blank**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Radar officer signature**

Restrictions:

Description: **Not used by TSLED or adjudication**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0

</Radar_Officer_Signature>

</PrdHeader>

<Motorist>

Description: **Motorist**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

This element contains the following other elements:

<FirstName>

Description: **Motorist's First Name**
Sample data: SALLY

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **First Name**

Restrictions:

Description: **Alpha characters and '-' (dash) are valid. The dash cannot be the first or last character. It is required for M or F gender code and Not required for gender of C for corporation.**

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 0**
 - **xsd:maxLength: 20**

</FirstName>

<MI>

Description: **Motorist's Middle Initial, or Middle Name**
Sample data: D

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Middle Initial, or Middle Name**

Restrictions:

Description: **Must be alpha-only**

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 0**
 - **xsd:maxLength: 20**

</MI>

<LastName>

Description: **Motorist's Last Name**
 Sample data: **SAMPLE**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Last Name**

Restrictions:

Description: **Last Name can only contain alpha characters, '-' (dash), and '.' (periods). The dash cannot be the first or last position. The period can only be in the 3rd position following ST.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 0
- **xsd:maxLength:** 20

</LastName>

<Suffix>

Description: **Motorist's Suffix**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Suffix Name: If supplied, must be one of the DMV acceptable suffixes**

Restrictions:

- **type:** NameSuffixType

Description: **Suffix**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 0
- **xsd:maxLength:** 5

Data table:

Value:	Literal:
II	II
III	III

Electronic Ticket/Accident Reporting Specifications

IV	IV
JR	JR
SR	SR
2	2
2ND	2ND
3	3
3RD	3RD
4	4
4TH	4TH
5	5
5TH	5TH
6	6
6TH	6TH

</Suffix>

<StreetAddress>

Description: **Motorist's Residence Street Address**
Sample data: 1010 ANYPLACE ST

Restrictions:

- minOccurs: 1 *** Required ***
- maxOccurs: 1

Description: **Street Address**

Restrictions:

Description: **Alpha numeric or '&' or '/' or '%' or '-' or spaces are the only valid entries**

Data must adhere to the following:

Restrictions:

- base: xsd:string
- xsd:minLength: 0
- xsd:maxLength: 20

</StreetAddress>

<City>

Description: **Motorist's Residence City**
Sample data: YOURCITY

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Residence City**

Restrictions:

Description: **Alpha or '-' or spaces are the only valid characters**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 20

</City>

<State>

Description: **Motorist's Residence State**
Sample data: NY

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **State or province**

Restrictions:

- **type:** StateType

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA

Electronic Ticket/Accident Reporting Specifications

BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI

Electronic Ticket/Accident Reporting Specifications

MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA

Electronic Ticket/Accident Reporting Specifications

TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<ZipCode>

Description: **Motorist's Residence Zip-Code**
Sample data: 12121

Restrictions: **minOccurs: 1 *** Required *****
maxOccurs: 1

Description: **Zip-Code**

Restrictions: **type: FormatZipCodeType**
Data must adhere to the following:
 Restrictions: **base: xsd:string**
xsd:pattern: [0-9]{5}(-[0-9]{4})?
xsd:minLength: 5
xsd:maxLength: 10

</ZipCode>

<DateOfBirth>

Electronic Ticket/Accident Reporting Specifications

Description: **Motorist's Birth Date: If the Gender is Male or Female, the date of birth (DOB) of the motorist is required**
Sample data: 7/18/1993

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Birth date**

- Restrictions:
- **type:** DateTracsType

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 8
 - **xsd:maxLength:** 10

</DateOfBirth>

<DateExpires>

Description: **License Expiration Date**
Sample data: 7/18/2013

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **License Expiration Date**

- Restrictions:
- **type:** DateTracsType

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 8
 - **xsd:maxLength:** 10

</DateExpires>

<Gender>

Description: **Motorist's Gender (Code)**

Sample data: F

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Gender**

- Restrictions:
- **type: GenderType**

Description: **Gender**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 1**
 - **xsd:maxLength: 1**

Data table:

Value:	Literal:
M	Male
F	Female
C	Corporation
U	Unknown

</Gender>

<License>

Description: **License. Required if there is a license present.**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Driver's license**

- Restrictions:
- **type: MotoristLicenseType**

Description: **Motorist License**

This element contains the following other elements:

<Number>

Description: **Drivers License Number**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Out Of State License Number or NY Client Id**
Sample data: 000000000

Restrictions:

Description: **If the accused is not a corporation, and the motorist is licensed in a state other than NY, this would be the motorist's license number from the issuing state. If unlicensed, this field should be left blank. Format: Alphanumeric Only, 25 character maximum. If the accused is not a corporation, and the motorist's license is from NY this should be the NYS Client-Id from their license. This is always a nine-numeric, never (000000000) or (555555555) or (999999999), 9 character maximum length. If unknown or unlicensed, this field should be left blank.**

Data must adhere to the following:

Description: **A minimum length of zero allows the element to be left blank.**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 0
 - **xsd:maxLength:** 25

</Number>

<State>

Description: **State license issued in. Required if there is a license present**
Sample data: NY

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **State or province**

Restrictions:

- **type:** StateType

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Electronic Ticket/Accident Reporting Specifications

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS
KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS

Electronic Ticket/Accident Reporting Specifications

MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA
OR	OREGON
OT	OTHER

Electronic Ticket/Accident Reporting Specifications

PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<Class>

Description:

License Class

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **License Class: If the accused is a licensed motorist from another state, then the Class of the motorist's license is required. If the motorist is not licensed or the class of the motorist's license cannot be determined, the default should be "UNK"**
Sample data: B

Restrictions: **• type: LicenseClassType**

Description: **Conditional - If the accused is a licensed motorist from another state, then the Class of the motorist's license is required. If the motorist is not licensed or the class of the motorist's license cannot be determined, the default should be "UNK".**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions: **• base: xsd:string**
• xsd:maxLength: 3

Data table:

Value:	Literal:
A	Commercial, Class A: Commercial, Class A, Class B and Class C (CDL): Drivers age 21 or over can apply for a Class A driver license or any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR)

Electronic Ticket/Accident Reporting Specifications

	of 26,001 lbs. or more.
B	Commercial, Class B: Commercial, Class A, Class B and Class C (CDL): Drivers age 21 or over can apply for a Class A driver license or any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR) of 26,001 lbs. or more.
C	Commercial, Class C:Commercial, Class A, Class B and Class C (CDL): Drivers age 21 or over can apply for a Class A driver license or any CDL with a hazardous materials endorsement. Drivers age 18 or over can apply for a Class B or Class C driver license. Valid for the same vehicles that a Class E driver can drive plus buses and trucks that have a gross vehicle weight rating (GVWR) of 26,001 lbs. or more.
D	Operator, Class D:

Electronic Ticket/Accident Reporting Specifications

	<p>Issued to drivers age 18 or over, or to drivers age 17 with Driver Education. Valid for passenger cars and trucks with a gross vehicle weight rating (GVWR) of 26,000 lbs. or less. A Class D driver can drive a vehicle that tows another vehicle (for example a trailer) that has a maximum gross weight of 10,000 lbs. or less. A Class D driver can tow a vehicle with a GVWR of more than 10,000 lbs only if the combined weight rating of the two vehicles is 26,000 lbs. or less.</p>
E	<p>Taxi and Livery, Class E: Issued to drivers age 18 or over. Valid for the same vehicles that a class D driver can drive, plus for-hire vehicles that carry 14 passengers or less.</p>
DJ	<p>Junior License, Class DJ: Issued to drivers under the age of 18, with restrictions. Read the DMV brochure, Learner Permits and Junior Licenses. Valid for passenger cars and trucks with a gross</p>

	vehicle weight rating (GVWR) of 10,000 lbs. or less. A class DJ driver can drive a vehicle that tows another vehicle (for example a trailer) with a GVWR of 3,000 lbs. or less.
M	Motorcycle, Class M: for motorcycles.
MJ	Junior Motorcycle License, Class MJ: for motorcycle drivers under the age of 18, with restrictions.
NC	Non-CDL Class C: Changes for Class D drivers resulted from a law that eliminates the Non-CDL Class C license.
UNK	Unknown: If the motorist is not licensed or the class of the motorist's license cannot be determined.

Data must adhere to the following:

Description: **For out-of-state licenses, enter the class from the license up to a maximum of three characters**

Restrictions: **• base: xsd:string
• xsd:maxLength: 3**

</Class>
</License>

</Motorist>

<Vehicle>

Description: **Vehicle**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Vehicle information**

This element contains the following other elements:

<PlateNumber>

Description: **Plate Number**
Sample data: 123ABC

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **Plate Number**

Restrictions:

Description: **Alphanumeric plate number with no embedded spaces or special characters.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 8

</PlateNumber>

<PlateState>

Description: **Registration State**
Sample data: NY

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **State vehicle is registered in**

Restrictions:

- **type:** StateType

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS

Electronic Ticket/Accident Reporting Specifications

KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA

Electronic Ticket/Accident Reporting Specifications

OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</PlateState>

<RegistrationType>

Description: **Registration Type**
 Sample data:

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Registration type: Required with certain Registration violations**

- Restrictions:
- **type:** VehicleRegistrationTypeType

Description: **Vehicle Registration Type**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 3

Data table:

Value:	Literal:
AGC	Agricultural Commercial
AGR	Agricultural
AMB	Ambulance
ARG	Air National Guard
ATD	All Terrain Dealer
ATV	All Terrain Vehicle
AYG	Army National Guard
BOB	Birthplace of Baseball
BOT	Boats
CBS	County Board of Supervisors
CCK	County Clerk
CHC	Household Carrier Commercial
CLG	County Legislators
CME	Coroner/Medical Examiner
CMH	Congressional Medal of Honor
COM	Commercial
CSP	Sports Commercial
DLR	Dealer

Electronic Ticket/Accident Reporting Specifications

FAR	Farm
FPW	Former Prisoner of War
GSM	Gold Star Mothers
HAC	Ham Operator Commercial
HAM	Ham Operator
HIF	Special Reg Hearse
HIR	Hearse Coach (Hearse/Invalid Regular)
HIS	Historical
HOU	House or Coach Trailer
HSM	Historical Motorcycle
IRP	International Reg Plan
ITP	In Transit Permit
JCA	Court of Appeals
JCL	Court of Claims
JSC	Supreme Court (ADJ)
JWV	Jewish War Veterans
LMA	Limited Use Motorcycle - Type A
LMB	Limited Use Motorcycle - Type B
LMC	Limited Use Motorcycle - Type C
LOC	Locomotive
LTR	Light Trailer
LUA	Limited Use Automobile
MCD	Motorcycle dealer
MCL	Marine Corp League
MED	Medical Doctor
MOT	Motorcycle
NLM	Naval Militia
NYA	New York State Assembly

Electronic Ticket/Accident Reporting Specifications

NYC	New York Council
NYS	New York State Senate
OMF	(Public Service) Omnibus
OML	(Livery) Omnibus
OMO	Omnibus Out-of-State
OMR	(Regular) Omnibus
OMS	(Special) Omnibus (Rentals)
OMT	(Taxi) Omnibus
OMV	(Vanity) Omnibus (Rentals)
ORC	Organizational Commercial
ORG	Organizational
ORM	Organizational Motorcycle
PAS	Passenger (Passenger)
PHS	Pearl Harbor Survivors
PPH	Purple Heart
PSD	Political Subdivision (municipal/thruway)
RGC	Regional Commercial
RGL	Regional
SCL	School Car
SEM	Commercial Semi-Trailer
SNO	Snowmobiles
SOS	Survivors of the shield
SPC	Special Purpose Commercial
SPO	Sports (Passenger)
SRF	Special Passenger
SRN	Special Passenger (Judges/Officials)
STA	State Agencies
STG	State National Guard

Electronic Ticket/Accident Reporting Specifications

SUP	Supreme Court Justice
THC	Household Carrier Tractor
TOW	Tow Truck
TRA	Transporter
TRC	(Regular) Tractor
TRL	(Regular) Trailer
USC	U.S. Congress
USS	U.S. Senate
VAS	Volunteer Ambulance Services
VPL	Van Pool
WUG	World University Games

</RegistrationType>

<VehicleType>

Description: **Vehicle Type: Type of vehicle the defendant was driving or occupying at the time of the offense. Used to validate certain violations. Default: 1 Passenger**
Sample data: 1

Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1

Description: **Vehicle TypeDefault: 1 Passenger**

Restrictions: **• type: VehicleTypeType**

Description: **Type of vehicle**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions: **• base: xsd:string**
• xsd:minLength: 1
• xsd:maxLength: 1

Data table:

Value:	Literal:
0	No vehicle
1	Passenger

Electronic Ticket/Accident Reporting Specifications

2	Bus
3	Motorcycle
4	Moped
5	Truck
6	Truck/Tractor
7	Recreation vehicle
8	Farm vehicle
9	All others
A	All terrain vehicle
B	Bicycle
P	Pick up truck
V	Van

</VehicleType>

<Make>

Description: **Vehicle Make**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Vehicle Make**

- Restrictions:
- **type: VehicleMakeType**

Description: **Maximum of 5 character Vehicle Make**

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**
 - **xsd:minLength: 1**
 - **xsd:maxLength: 5**

Data table:

Value:	Literal:
-3	Not Entered
-2	Not Applicable
-1	Unknown Make

Electronic Ticket/Accident Reporting Specifications

1	American Motors*
2	Jeep* (Includes Willys/Kaiser-Jeep)
3	AM General
4	Chrysler/DaimlerChrysler
5	Dodge
6	Imperial
7	Plymouth
8	Eagle*
9	Ford
10	Lincoln
11	Mercury
12	Buick
13	Cadillac
14	Chevrolet
15	Oldsmobile
16	Pontiac
17	GMC
18	Saturn
19	Grumman/Grumman-Olson
20	Other Domestic Manufacturers
21	Volkswagen
22	Alfa Romeo
23	Audi
24	Austin/Austin Healey
25	BMW
26	Nissan/Datsun
27	Fiat
28	Honda

Electronic Ticket/Accident Reporting Specifications

29	Isuzu
30	Jaguar
31	Lancia
32	Mazda
33	Mercedes-Benz
34	MG
35	Peugeot
36	Porsche
37	Renault
38	Saab
39	Subaru
40	Toyota
41	Triumph
42	Volvo
43	Mitsubishi
44	Suzuki
45	Acura
46	Hyundai
47	Merkur
48	Yugo
49	Infiniti
50	Lexus
51	Daihatsu
52	Sterling
53	Land Rover
54	KIA
55	Daewoo
56	Other Import

Electronic Ticket/Accident Reporting Specifications

57	BSA
58	Ducati
59	Harley-Davidson
60	Kawasaki
61	Moto-Guzzi
62	Norton
63	Yamaha
64	Brockway
65	Diamond Reo or Reo
66	Freightliner
67	FWD
68	International Harvester/Navistar
69	Kenworth
70	Mack
71	Peterbilt
72	Iveco/Magirus*
73	White/Autocar-WhiteGMC
74	Bluebird
75	Eagle Coach
76	Gillig
77	MCI
78	Thomas Built
79	Other Make *

</Make>

<Year>

Description: **Vehicle Year**
Sample data: 1997

Restrictions: **• minOccurs: 1 *** Required *****
• maxOccurs: 1

Electronic Ticket/Accident Reporting Specifications

Description: **Vehicle Year**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 4
 - **xsd:maxLength:** 4

</Year>

<RegExpires>

Description: **Registration Expiration**
Sample data: 6/30/2006

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Registration Expiration Date**

Restrictions: • **type:** DateTracsType

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 8
 - **xsd:maxLength:** 10

</RegExpires>

<VehColor>

Description: **Vehicle Color**
Sample data: BK

- Restrictions:
- **minOccurs:** 1 *** Required ***
 - **maxOccurs:** 1

Description: **Vehicle Color**

Restrictions: • **type:** VehicleColorType

Data must adhere to the following:

Description: **When vehicle information is returned in a batch registration inquiry, the color of the vehicle will be represented by the elements**

DMV_VEH_COLOR1_CDE and DMV_VEH_COLOR2_CDE.

The following table lists the codes that may be returned to indicate the color of a registered vehicle:

Color Codes

Standard Color Codes : (may be returned as Color1 or Color2)

BK: Black	OR: Orange
BL: Blue	PK: Pink
BR: Brown	PR: Purple
GL: Gold	RD: Red
GR: Green	TN: Tan
GY: Gray	WH: White
MR: Maroon	YW: Yellow

Special Color Codes : (see “Color Combinations” for more information)

DK Dark	- Used to modify a standard color. Can be returned only as Color1
LT Light	- Used to modify a standard color. Can be returned only as Color1
NO No	- Can be returned only as Color1, and only if paired with “CL”
CL Color	- Can be returned only as Color2, and only if paired with “NO”.

Color Combinations

If both Color1 and Color2 are returned, it will be necessary to examine both codes to determine the meaning:

- If both Color1 and Color2 are “standard colors” as listed in the table above, then it means that the vehicle is painted in those two colors.
- If Color1 is “DK” or “LT”, then the vehicle is painted a dark or light shade of the color indicated in Color2.
- If Color1 is “NO” and Color2 is “CL”, it means that the DMV file does not have any color information for the vehicle (i.e., the color of the vehicle is unknown).

Here are some example combinations:

Color1	Color2	Interpretation
RD	BK	Red and Black
DK	GY	Dark Gray
LT	GR	Light Green
NO	CL	No color (color unknown)

Restrictions:

- **base:** xsd:string

</VehColor>

<RegisteredWeight>

Description: **Registered vehicle Weight**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Registered vehicle Weight**

Restrictions:

Description: **Required for weight violations. See Conditional Table.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:maxLength:** 6

</RegisteredWeight>

<NumberOfAxles>

Electronic Ticket/Accident Reporting Specifications

Description: **Number of Axles**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Number of Axles**

Restrictions:

Description: **Required for certain Registration Violations. See Conditional Table.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 2

</NumberOfAxles>

<Commercial>

Description: **Commercial vehicle indicator**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Commercial vehicle indicator**

- Restrictions:
- **type:** CommercialVehicleIndicatorType

Description: **Values "Y" If the Vehicle is Commercial, "N" if not commercial.**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
Y	Commercial Vehicle
N	Not commercial vehicle

</Commercial>

<Bus>

Description: **Bus Indicator**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Electronic Ticket/Accident Reporting Specifications

Description: **Bus Indicator**

Restrictions:

- **type:** BusIndicatorType

Description: **Values "Y" If the Vehicle is a Commercial Bus, "N" if not a bus**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
Y	Bus
N	Not a bus

</Bus>

<HazardousMaterial>

Description: **HazMat Indicator**

Restrictions:

- **minOccurs:** 1 *** Required ***
- **maxOccurs:** 1

Description: **HazMat Indicator**

Restrictions:

- **type:** HazardousMaterialIndicatorType

Description: **Values: "Y" If the Vehicle is carrying Hazardous Materials or Placarded as such, or "N" if not**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
Y	Haz Mat
N	Non HazMat vehicle

</HazardousMaterial>

<OwnerOwned>

Electronic Ticket/Accident Reporting Specifications

Description: **Owner owned**
Sample data: **1**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Owner owned**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**
- **xsd:maxLength: 1**

</OwnerOwned>

<DOTNumber>

Description: **US Dot Number**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **US Dot Number**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**
- **xsd:maxLength: 8**

</DOTNumber>

</Vehicle>

<Court>

Description: **Court**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

This element contains the following other elements:

<Code>

Description: **DCJS Court Code - ORI Number: Court code that the ticket is answerable to**
Sample data: **NY031121J**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Electronic Ticket/Accident Reporting Specifications

Description: **DCJS Court Code - ORI Number: Court code that the ticket is answerable to**

Restrictions: **• type: CourtCodeType**

Description: **Court code must either be on the list for valid adjudication courts or a valid ORI number**

Description: **Adjudication court codes**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:maxLength:** 7

Data table:

Value:	Literal:
TVB1499	TVB1499
TVB2799	TVB2799
TVB5199	TVB5199
TVB7050	TVB7050
TVB7111	TVB7111
TVB7150	TVB7150
TVB7211	TVB7211
TVB7250	TVB7250
TVB7311	TVB7311
TVB7350	TVB7350
TVB7550	TVB7550

Description: **Valid ORI Number**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:pattern:** [N][Y][0-9]{6}[J]
 - **xsd:minLength:** 9
 - **xsd:maxLength:** 9

</Code>

<StreetAddress>

Description: **Court Street Address**

Electronic Ticket/Accident Reporting Specifications

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Street Address**

Restrictions:

Description: **Alpha numeric or '&' or '/' or '%' or '-' or spaces are the only valid entries**

Data must adhere to the following:

Restrictions: • **base:** xsd:string
 • **xsd:minLength:** 0
 • **xsd:maxLength:** 20

</StreetAddress>

<City>

Description: **Court City**

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Residence City**

Restrictions:

Description: **Alpha or '-' or spaces are the only valid characters**

Data must adhere to the following:

Restrictions: • **base:** xsd:string
 • **xsd:minLength:** 0
 • **xsd:maxLength:** 20

</City>

<State>

Description: **Court State: Must be set to NY**

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **State or province**

Restrictions: • **type:** StateType

Description: **List of US States and Canadian Provinces**

Data must adhere to the following:

Description: **Select an option from the list**

Electronic Ticket/Accident Reporting Specifications

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

Data table:

Value:	Literal:
AB	ALBERTA, CANADA
AK	ALASKA
AL	ALABAMA
AR	ARKANSAS
AS	AMERICAN SAMOA
AZ	ARIZONA
BC	BRITISH COLUMBIA, CANADA
CA	CALIFORNIA
CO	COLORADO
CT	CONNECTICUT
DC	DISTRICT OF COLUMBIA
DE	DELAWARE
FL	FLORIDA
FO	FOREIGN LICENSE
GA	GEORGIA
GL	US GOVERNMENT LICENSE
GM	GUAM
HI	HAWAII
IA	IOWA
ID	IDAHO
IL	ILLINOIS
IN	INDIANA
IT	INTERNATIONAL LICENSE
KS	KANSAS

Electronic Ticket/Accident Reporting Specifications

KY	KENTUCKY
LA	LOUISIANA
MA	MASSACHUSETTS
MB	MANITOBA, CANADA
MD	MARYLAND
ME	MAINE
MI	MICHIGAN
MN	MINNESOTA
MO	MISSOURI
MS	MISSISSIPPI
MT	MONTANA
MX	MEXICO
NB	NEW BRUNSWICK, CANADA
NC	NORTH CAROLINA
ND	NORTH DAKOTA
NE	NEBRASKA
NF	NEWFOUNDLAND, CANADA
NH	NEW HAMPSHIRE
NJ	NEW JERSEY
NM	NEW MEXICO
NS	NOVA SCOTIA, CANADA
NT	NORTHWEST TERRITORIES, CANADA
NU	NUNAVUT, CANADA
NV	NEVADA
NY	NEW YORK
OH	OHIO
OK	OKLAHOMA
ON	ONTARIO, CANADA

Electronic Ticket/Accident Reporting Specifications

OR	OREGON
OT	OTHER
PA	PENNSYLVANIA
PE	PRINCE EDWARD ISLAND, CANADA
PR	PUERTO RICO
QC	QUEBEC, CANADA
RI	RHODE ISLAND
SC	SOUTH CAROLINA
SD	SOUTH DAKOTA
SK	SASKATCHEWAN, CANADA
TN	TENNESSEE
TX	TEXAS
UN	UNLICENSED/UNREGISTERED
US	US GOVERNMENT/ FOREIGN DIPLOMATS
UT	UTAH
VA	VIRGINIA
VI	VIRGIN ISLANDS
VT	VERMONT
WA	WASHINGTON
WI	WISCONSIN
WV	WEST VIRGINIA
WY	WYOMING
YT	YUKON, CANADA
ZS	ANY AREA NOT COVERED

</State>

<ZipCode>

Description: **Court Zip Code**

Restrictions: **• minOccurs: 0**

Electronic Ticket/Accident Reporting Specifications

• **maxOccurs:** 1

Description: **Zip-Code**

Restrictions:

- **type:** FormatZipCodeType

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:pattern:** [0-9]{5}(-[0-9]{4})?
- **xsd:minLength:** 5
- **xsd:maxLength:** 10

</ZipCode>

<CourtDate>

Description: **Appearance Date: The date, by which, the motorist is ordered to answer the charge on the ticket. If this date is in an incorrect format, missing, more than a year in the future or prior to the violation date an Exception will be generated**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Appearance Date: The date, by which, the motorist is ordered to answer the charge on the ticket. If this date is in an incorrect format, missing, more than a year in the future or prior to the violation date an Exception will be generated**

Restrictions:

- **type:** DateTracsType

Description: **Date**

Data must adhere to the following:

Description: **MM/DD/YYYY: format. Do not zero fill months and days. July 4 should be 7/4 NOT 07/04.**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 8
- **xsd:maxLength:** 10

</CourtDate>

<CourtTime>

Description: **Appearance Time: The time at which the motorist is ordered to answer the charge on the ticket**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Appearance Time**

Restrictions:

Data must adhere to the following:

Description: **Must match the pattern: HH:MM using the 24 hour clock**

- Restrictions:
- **base:** xsd:string
 - **xsd:pattern:** [0-2]{1}[0-9]{1};[0-5]{1}[0-9]{1}
 - **xsd:minLength:** 5
 - **xsd:maxLength:** 5

</CourtTime>

<DWITest>

Description: **DWI Test. Alcohol and Drug tests and results data is required in the violation section**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **DWI Test**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</DWITest>

<TestType>

Description: **Test type: Alcohol and Drug tests and results data is required in the violation section**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Test type**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</TestType>

<TestResults>

Description: **Test results: Alcohol and Drug tests and results data is required in the violation section**

Electronic Ticket/Accident Reporting Specifications

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Test results**

Restrictions:

Description: **Note: Alcohol and Drug tests and results data is required in the violation section.**

Data must adhere to the following:

 Restrictions: • **base:** xsd:string

</TestResults>

<OfficerNotes>

Description: **Officer Notes**

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Officer Notes. This element is not currently used.**

Restrictions:

Data must adhere to the following:

 Restrictions: • **base:** xsd:string

</OfficerNotes>

<ReturnByMail>

Description: **Return By Mail**

Restrictions: • **minOccurs:** 0
 • **maxOccurs:** 1

Description: **Return By Mail**

Restrictions:

Data must adhere to the following:

 Restrictions: • **base:** xsd:string

</ReturnByMail>

</Court>

<SupportingDeposition>

Description: **Supporting Deposition**

Restrictions: • **minOccurs:** 0

- **maxOccurs: 1**

This element contains the following other elements:

<Type>

Description: **Type of deposition**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Type of supporting deposition**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**

</Type>

<Information>

Description: **Information**

- Restrictions:
- **minOccurs: 1 *** Required *****
 - **maxOccurs: 1**

Description: **Information on supporting deposition**

Restrictions:

Description: **Used for exceptions**

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**
 - **xsd:maxLength: 500**

</Information>

<DefendantStatement>

Description: **Type of deposition**

- Restrictions:
- **minOccurs: 0**
 - **maxOccurs: 1**

Description: **Type of deposition**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base: xsd:string**

</DefendantStatement>

<ChargeBased>

Description: **Charge Based**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Charge Based**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</ChargeBased>

<DirectionTravel>

Description: **Direction of Travel**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Direction of Travel**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</DirectionTravel>

</SupportingDeposition>

<Violation>

Description: **Violation**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

This element contains the following other elements:

<ViolationDate>

Description: **Date and time of violation**
Sample data: 12/18/200508:01:00

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Electronic Ticket/Accident Reporting Specifications

Description: **Date and time of violation**

Restrictions:

- **type:** DateTimeTracsType

Description: **Date and time of the occurrence of the violation. Format: MM/DD/YYYYHH:MM:SS OR MM/DD/YYYY HH:MM:SS The Violation date cannot be in the future and cannot be more than 2 years old.**

Data must adhere to the following:

- Restrictions:
 - **base:** xsd:string
 - **xsd:minLength:** 13
 - **xsd:maxLength:** 22

</ViolationDate>

<TypeOfLaw>

Description: **Law Type: The type of law the section the violation charged is based on, as printed on the motorists' copy of the ticket (should match the first 3 characters of the DCJSCode)**
Sample data: VTL

Restrictions:

- **minOccurs:** 1 *** Required ***
- **maxOccurs:** 1

Description: **Law Type**

Restrictions:

- **type:** TypeOfLawType

Description: **The type of law**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
 - **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 3

Data table:

Value:	Literal:
PL	Penal Law
TAX	Tax Law
TL	Transportation Law
VTL	Vehicle/Traffic Law

</TypeOfLaw>

Electronic Ticket/Accident Reporting Specifications

<DCJSCode>

Description: **DCJS Law Code: DCJS Encoded Violation Code for Violation Charged**
Sample data: VTL0375 31 0I0

Restrictions:

- minOccurs: 1 *** Required ***
- maxOccurs: 1

Description: **DCJS Law Code**

Restrictions:

Description: **DCJS Encoded Violation Code for Violation Charged. (see Violation Codes table)**

Data must adhere to the following:

Restrictions:

- base: xsd:string
- xsd:minLength: 1
- xsd:maxLength: 22

</DCJSCode>

<ActualSpeed>

Description: **Actual Speed Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater than 5 and less than 200. Must be greater than speed zone.**

Restrictions:

- minOccurs: 0
- maxOccurs: 1

Description: **Actual Speed**

Restrictions:

Description: **Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater than 5 and less than 200. Must be greater than speed zone.**

Data must adhere to the following:

Restrictions:

- base: xsd:integer
- xsd:minExclusive: 5
- xsd:maxExclusive: 200

</ActualSpeed>

<ZoneSpeed>

Description: **Zone Speed - Posted Limit: Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater or equal to 5 and less than or equal to 65 in multiples of 5. Must be less than actual speed.**

Restrictions:

- minOccurs: 0

Electronic Ticket/Accident Reporting Specifications

• **maxOccurs:** 1

Description: **Zone Speed - Posted Limit**

Restrictions:

Description: **Required for violations of sections 1180B, 1180C, 1180D, 1180D2, 1180F and 1180G. Must be greater or equal to 5 and less than or equal to 65 in multiples of 5. Must be less than actual speed.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:integer
- **xsd:minInclusive:** 5
- **xsd:maxInclusive:** 65

</ZoneSpeed>

<HighwayTypeCode>

Description: **Highway Type: Type of road the violation occurred on**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Highway Type: Type of road the violation occurred on**

Restrictions:

- **type:** HighwayTypeCodeType

Description: **Type of road**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Interstate
2	State highway
3	County
4	Town
5	Village
6	City
7	Off road

Electronic Ticket/Accident Reporting Specifications

8	Parking lot
9	Parkway

</HighwayTypeCode>

<RouteCode>

Description: **Route Code**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Route Code**

Restrictions:

Description: **If the Highway type is 1(Interstate), 2(State highway) or 9(Parkway) the route code is required, otherwise it is optional. - Type 9 is per TSLED Lookup (parkway)**

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 4

Data table:

Value:	Literal:
BDPK	Bay Drive
BRPK	Bronx River Parkway
BSPK	Bethpage State Parkway
CCPK	Cross County Parkway
HRPK	Hutchinson River Parkway
HSPK	Heckscher Spur
LMPK	Long Mountain Parkway
LOPK	Lake Ontario State Parkway
LPKY	Loop Parkway
MCPK	Robert Moses Causeway
MSPK	Meadowbrook Parkway
NSPK	Northern State Parkway

Electronic Ticket/Accident Reporting Specifications

OCPK	Ocean Parkway
PIPK	Palisades Interstate Parkway
RMPK	Robert Moses Parkway
SAPK	Sagtikos State Parkway
SBPK	Sprain Brook Parkway
SMPK	Saw Mill River Parkway
SOPK	South State Parkway
SSPK	Southern State Parkway
SUPK	Sunken Meadow Spur
TSPK	Taconic State Parkway
UNKN	Unknown
WRPK	W. River St Parkway
WSPK	Wantagh State Parkway

</RouteCode>

<MuniCode>

Description: **Muni Code: 4-digit municipality code where the violation occurred. Should agree with the municipalities the NCIC can write tickets to and the municipalities answerable to the court**

Restrictions: **• minOccurs: 0**
• maxOccurs: 1

Description: **Muni Code**

Restrictions:

Description: **4-digit municipality code where the violation occurred. Should agree with the municipalities the NCIC can write tickets to and the municipalities answerable to the court - per TSLED Lookups.**

Data must adhere to the following:

Restrictions: **• base: xsd:string**
• xsd:minLength: 4
• xsd:maxLength: 4

</MuniCode>

<ArrestTypeCode>

Electronic Ticket/Accident Reporting Specifications

Description: **Arrest Type**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Arrest Type**

Restrictions:

Description: **Per TSLED Lookup - Arrest Type Will default to the code for “Unknown” if the data is not present or not on database Arrest_Type table. This field serves as the indicator as to whether the charge is based on a property, personal injury or fatal accident.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Patrol
2	Radar
3	Road check
4	Scales
5	Property damage accident
6	Personal injury accident
7	Fatal accident
8	Aircraft
9	Other
L	Laser
V	Vascar
W	Work zone

</ArrestTypeCode>

<ArrestTransactionDate>

Description: **Arrest Transaction Date**

Restrictions:

- **minOccurs:** 0

Electronic Ticket/Accident Reporting Specifications

- **maxOccurs:** 1

Description: **Arrest Transaction Date**

Restrictions:

- **type:** DateTimeTracsType

Description: **Date and time of the occurrence of the violation. Format: MM/DD/YYYYHH:MM:SS OR MM/DD/YYYY HH:MM:SS The Violation date cannot be in the future and cannot be more than 2 years old.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 13
- **xsd:maxLength:** 22

</ArrestTransactionDate>

<LocalOffice>

Description: **Local Office - TZS: For State Police, this field is the Troop/Zone/Sector(TZS). For others, this can be a precinct or sub station.**
Sample data: A111

Restrictions:

- **minOccurs:** 1 *** Required ***
- **maxOccurs:** 1

Description: **Local Office - TZS**

Restrictions:

Description: **For State Police, this field is the Troop/Zone/Sector(TZS). For others, this can be a precinct or sub station.**

Data must adhere to the following:

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 4

</LocalOffice>

<PoliceAgency>

Description: **NCIC Description: Used for exceptions**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **NCIC Description**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 30

</PoliceAgency>

<CTVName>

Description: **CTV Name**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **CTV Name**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</CTVName>

<PlaceOfOccurance>

Description: **Place Of Occurance**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Place Of Occurance**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</PlaceOfOccurance>

<DriverLicShown>

Description: **Driver's License Shown**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Driver's License Shown**

Restrictions:

Data must adhere to the following:

- Restrictions:
- **base:** xsd:string

</DriverLicShown>

<ViolationDescription>

Description: **Violation Description**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Violation Description**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base: xsd:string**

</ViolationDescription>

<LawSection>

Description: **VT Code: Violation Charged - Must match DMV violation code table.
Sample data: 3752A1**

Restrictions:

- **minOccurs: 1 *** Required *****
- **maxOccurs: 1**

Description: **VT Code**

Restrictions:

Description: **Violation Charged - Must match DMV violation code table.**

Data must adhere to the following:

Restrictions:

- **base: xsd:string**
- **xsd:minLength: 1**
- **xsd:maxLength: 7**

</LawSection>

<Ordinal>

Description: **Ordinal
Sample data: 06600**

Restrictions:

- **minOccurs: 0**
- **maxOccurs: 1**

Description: **Ordinal**

Restrictions:

Data must adhere to the following:

Restrictions:

- **base:** xsd:string

</Ordinal>

<AlcoholDrugTest>

Description: **Alcohol-Drug test Administered Code**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Alcohol-Drug test Administered Code**

Restrictions:

- **type:** AlcoholDrugTestAdministeredType

Description: **If 1192.X (Drug or alcohol related offense) a code indicating whether a test for alcohol or drugs was given**

Data must adhere to the following:

Description: **Select an option from the list**

Restrictions:

- **base:** xsd:string
- **xsd:minLength:** 1
- **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Test given, results required
2	Test refused
3	No test given
4	Unknown if test was given

</AlcoholDrugTest>

<AlcoholDrugTestType>

Description: **Alcohol-Drug Test Type Code**

Restrictions:

- **minOccurs:** 0
- **maxOccurs:** 1

Description: **Alcohol-Drug Test Type Code**

Restrictions:

- **type:** AlcoholDrugTestTypeType

Description: **If 1192.X, and a test for alcohol or drugs was administered, a code of the type of test**

Data must adhere to the following:

Description: **Select an option from the list**

- Restrictions:
- **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
1	Breathalyzer
2	Blood test
3	Urinalysis

</AlcoholDrugTestType>

<AlcoholTestResult>

Description: **Alcohol Test Result: If 1192.1,2,3,5,6 and a test for alcohol was administered, a two-digit number between 00 and 60, when multiplied by .10 is equal to the BAC of the test result.**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Description: **Alcohol Test Result**

Restrictions:

Description: **If 1192.1,2,3,5,6 and a test for alcohol was administered, a two-digit number between 00 and 60, when multiplied by .10 is equal to the BAC of the test result.**

Data must adhere to the following:

Description: **A two-digit number between 00 and 60**

- Restrictions:
- **base:** xsd:string
 - **xsd:pattern:** [0-6]{1}[0-9]{1}
 - **xsd:minLength:** 2
 - **xsd:maxLength:** 2

</AlcoholTestResult>

<DrugTestResult>

Description: **Drug Test Result**

- Restrictions:
- **minOccurs:** 0
 - **maxOccurs:** 1

Electronic Ticket/Accident Reporting Specifications

- Description: **Drug Test Result**
- Restrictions:
 - **type:** DrugTestResultType
- Description: **If 1192.4 and a test for drugs was administered**
- Data must adhere to the following:**
- Description: **Select an option from the list**
- Restrictions:
 - **base:** xsd:string
 - **xsd:minLength:** 1
 - **xsd:maxLength:** 1

Data table:

Value:	Literal:
P	Positive
N	Negative

</DrugTestResult>
</Violation>

- <Location>**
- Description: **Location: Not used by Adjudication**
- Restrictions:
 - **minOccurs:** 0
 - **maxOccurs:** 1

</Location>
</Ticket>
</Contents>
</File>

Accidents

Accident Report Case Number

In order to prevent duplicate Accident reporting numbers among the many agencies and locations across New York, a unique sequencing number, called a case number (data element 'case_number' in the 'Summary' file,) must be assigned. The case number will have a 12-character value with the following components:

pos	Description
1-2	The agency code as assigned by DMV
3-6	TraCS Sequence Numbering- (Modified Base 30) - Created by using the letters of the alphabet A-Z plus 0-9 characters minus vowels (A,E,I,O,U,Y) - Insures that the ticket will not spell or imply anything offensive - Recommend in place of using only numerics so more than 9999 tickets can be written
7-12	Machine code-This number MUST be UNIQUE within the issuing agency as it will become part of each Ticket and Accident Report number. The Criteria for the Machine Number is as follows: - Only letters and numbers are allowed, no special characters - All letters must be UPPER CASE - The machine number MUST be exactly 4 characters long - It can NOT start with Zero or the letter "O" - The 4th character MUST be a number - The first 3 characters of the machine number should not spell or imply anything offensive; the machine number is the first 4 characters of the Ticket number, and the third - sixth characters of the Accident Report number and as such will be seen by the public.

Case Number	Agency Code	Machine Code	Sequence Number
2T1L42000119	2T	1L42	000119
BWEG11000023	BW	EG11	000023

Data Input Schema

The following Schema illustrates the data element input 'tags' for accident reports.
(Note: Slight modification to the AIS schema is tentatively planned for June 2006.)

<Accident>

<Summary>

```

    <accident_date></accident_date>
    <accident_time></accident_time>
    <ammended></ammended>
    <badge></badge>
    <case_number></case_number>
    <CMV_fatal_injury></CMV_fatal_injury>
    <CMV_number_vehicle_person></CMV_number_vehicle_person>
    <CMV_qual_vehicles></CMV_qual_vehicles>
    <CMV_towed></CMV_towed>
    <CMV_transported></CMV_transported>
    <collision_direction></collision_direction>
    <cost_repair></cost_repair>
    <county></county>
    <ctv></ctv>
    <day></day>
    <fatal_indicator></fatal_indicator>
    <first_event></first_event>
    <formtypeA></formtypeA>
    <formtypeD></formtypeD>
    <formtypeS></formtypeS>
    <formversionA></formversionA>
    <formversionD></formversionD>
    <formversionS></formversionS>
    <investigated></investigated>
    <lanes></lanes>
    <leftscene></leftscene>
    <light_conditions></light_conditions>
    <loc_first_event></loc_first_event>
    <local_codes></local_codes>
    <ncicori></ncicori>
    <no_buses></no_buses>
    <no_hazmat_placard></no_hazmat_placard>
    <nonmotorist_action></nonmotorist_action>
    <nonmotorist_location></nonmotorist_location>
    <number_injured></number_injured>
    <number_killed></number_killed>
    <number_vehicle></number_vehicle>
    <officer_first></officer_first>

```

```

<officer_mi></officer_mi>
<officer_last></officer_last>
<officer_signature></officer_signature>
<Original_case_number></Original_case_number>
<photo></photo>
<Rank></Rank>
<reconstructed></reconstructed>
<reconstructed_shield></reconstructed_shield>
<review_date></review_date>
<review_officer_name></review_officer_name>
<review_officer_signature></review_officer_signature>
<review_time></review_time>
<road_surface_condition></road_surface_condition>
<roadway_character></roadway_character>
<roadway_flow></roadway_flow>
<roadway_surface></roadway_surface>
<speed_event></speed_event>
<station></station>
<traffic_control></traffic_control>
<troop></troop>
<truck_sixtires></truck_sixtires>
<tzs></tzs>
<weather_conditions></weather_conditions>
<work_related></work_related>
<zone></zone>
<Diagram></Diagram>
<LocToolVersion></LocToolVersion>
<CaptureDate></CaptureDate>
<XCoordinate></XCoordinate>
<YCoordinate></YCoordinate>
<ZCoordinate></ZCoordinate>
<at_intersection></at_intersection>
<distance_type></distance_type>
<intersection></intersection>
<location_definable></location_definable>
<literal_description></literal_description>
<location_direction></location_direction>
<location_distance></location_distance>
<loccounty></loccounty>
<map_version></map_version>
<reference_marker></reference_marker>
<road></road>
<SnapStatus></SnapStatus>
<narrative></narrative>
</Summary>

<Unit>
  <access_control></access_control>

```

<cargo_body></cargo_body>
 <carrier_explanation></carrier_explanation>
 <Carrier_Source></Carrier_Source>
 <CMV_first_event></CMV_first_event>
 <CMV_second_event></CMV_second_event>
 <CMV_third_event></CMV_third_event>
 <CMV_fourth_event></CMV_fourth_event>
 <Comm_Vehicle_Type></Comm_Vehicle_Type>
 <contr_cir_driver></contr_cir_driver>
 <contr_cir2_driver></contr_cir2_driver>
 <most_damaged_area></most_damaged_area>
 <damaged_area></damaged_area>
 <direction_travel></direction_travel>
 <estimated_speed></estimated_speed>
 <gross_weight></gross_weight>
 <hazmat_class_name></hazmat_class_name>
 <hazmat_code></hazmat_code>
 <hazmat_placard_info></hazmat_placard_info>
 <hazmat_released></hazmat_released>
 <hazmat_type></hazmat_type>
 <no_axles></no_axles>
 <overdimension_permit></overdimension_permit>
 <overweight_permit></overweight_permit>
 <point_impact></point_impact>
 <total_gross_weight></total_gross_weight>
 <total_occupants></total_occupants>
 <type_involved></type_involved>
 <unit_instance></unit_instance>
 <unknown_speed></unknown_speed>
 <vehicle_configuration></vehicle_configuration>
 <vehicle_long></vehicle_long>
 <vehicle_maneuver_action></vehicle_maneuver_action>
 <vehicle_towed_by></vehicle_towed_by>
 <vehicle_towed_to></vehicle_towed_to>
 <vehicle_towed></vehicle_towed>
 <vehicle_wide></vehicle_wide>
 <Year></Year>
 <Make></Make>
 <Model></Model>
 <VIN></VIN>
 <LicensePlate></LicensePlate>
 <LicenseState></LicenseState>
 <HazMatPlate></HazMatPlate>
 <VehRegType></VehRegType>
 <VehType></VehType>
 <CarrierName></CarrierName>
 <CarrierStreet></CarrierStreet>
 <CarrierCity></CarrierCity>

```

<CarrierState></CarrierState>
<CarrierZipCode></CarrierZipCode>
<CarrierDOTNumber></CarrierDOTNumber>
<CarrierICCNNumber></CarrierICCNNumber>
<Registrant_First_Name></Registrant_First_Name>
<Registrant_Middle_Name></Registrant_Middle_Name>
<Registrant_Last_Name></Registrant_Last_Name>
<Registrant_Sex></Registrant_Sex>
<Registrant_Street_Address_1></Registrant_Street_Address_1>
<Registrant_City></Registrant_City>
<Registrant_State></Registrant_State>
<Registrant_Zip_Code></Registrant_Zip_Code>
<Registrant_Birth_Date></Registrant_Birth_Date>
<HazMatCardReq></HazMatCardReq>
<second_event></second_event>
<owner_insurance></owner_insurance>
</Unit>

<Driver>
  <driver_airbag_not_vehicle></driver_airbag_not_vehicle>
  <driver_airbags_deployed></driver_airbags_deployed>
  <driver_condition></driver_condition>
  <CMV_driver_condition></CMV_driver_condition>
  <driver_date_death></driver_date_death>
  <driver_time_death></driver_time_death>
  <driver_deceased></driver_deceased>
  <driver_ejection></driver_ejection>
  <driver_injured></driver_injured>
  <driver_loc_complaint></driver_loc_complaint>
  <driver_Med_Facility></driver_Med_Facility>
  <hospital_information_name></hospital_information_name>
  <hospital_information_county></hospital_information_county>
  <hospital_information_state></hospital_information_state>
  <driver_other_hospital></driver_other_hospital>
  <driver_other_hospital_co></driver_other_hospital_co>
  <driver_other_hospital_state></driver_other_hospital_state>
  <driver_med_notified></driver_med_notified>
  <driver_med_arrived></driver_med_arrived>
  <driver_med_arrived_hospital></driver_med_arrived_hospital>
  <driver_owner_known></driver_owner_known>
  <driver_safety_system></driver_safety_system>
  <driver_seating_position></driver_seating_position>
  <driver_source_transport></driver_source_transport>
  <driver_type_complaint></driver_type_complaint>
  <extricated></extricated>
  <extrication_equipment></extrication_equipment>
  <unlicensed></unlicensed>
  <vio_charge1></vio_charge1>

```

```

<vio_charge2></vio_charge2>
<vio_charge3></vio_charge3>
<vio_charge4></vio_charge4>
<vio_charge5></vio_charge5>
<vio_charge6></vio_charge6>
<vio_number1></vio_number1>
<vio_number2></vio_number2>
<vio_number3></vio_number3>
<vio_number4></vio_number4>
<vio_number5></vio_number5>
<vio_number6></vio_number6>
<First></First>
<Middle></Middle>
<Last></Last>
<Street></Street>
<City></City>
<State></State>
<ZipCode></ZipCode>
<DOB></DOB>
<Age></Age>
<Gender></Gender>
<LicNumber></LicNumber>
<LicType></LicType>
<LicState></LicState>
<InsurCompany></InsurCompany>
<unit_instance></unit_instance>
</Driver>

<Passenger>
  <airbags_deployed></airbags_deployed>
  <airbags_not_vehicle></airbags_not_vehicle>
  <date_death></date_death>
  <deceased></deceased>
  <ejection></ejection>
  <extricated></extricated>
  <extrication_type></extrication_type>
  <injured></injured>
  <loc_complaint></loc_complaint>
  <med_arrived></med_arrived>
  <med_arrived_hospital></med_arrived_hospital>
  <hospital_information_name></hospital_information_name>
  <hospital_information_county></hospital_information_county>
  <hospital_information_state></hospital_information_state>
  <med_facility></med_facility>
  <med_notified></med_notified>
  <other_hospital></other_hospital>
  <other_hospital_co></other_hospital_co>
  <other_hospital_state></other_hospital_state>

```

```
<person_condition></person_condition>
<safety_equipment></safety_equipment>
<seating_position></seating_position>
<source_transport></source_transport>
<time_death></time_death>
<type_complaint></type_complaint>
<unit_no></unit_no>
<First></First>
<Middle></Middle>
<Last></Last>
<Street></Street>
<City></City>
<State></State>
<ZipCode></ZipCode>
<DOB></DOB>
<Age></Age>
<Gender></Gender>
</Passenger>

<PropertyDamage>
  <OwnerFirstName></OwnerFirstName>
  <OwnerMiddleInitial></OwnerMiddleInitial>
  <OwnerLastName></OwnerLastName>
  <OwnerStreetAddress></OwnerStreetAddress>
  <OwnerCity></OwnerCity>
  <OwnerState></OwnerState>
  <OwnerZip></OwnerZip>
  <Unit_Instance></Unit_Instance>
  <object_damaged></object_damaged>
  <owner_notified></owner_notified>
  <PrivatePropertyDamaged></PrivatePropertyDamaged>
  <PublicPropertyDamaged></PublicPropertyDamaged>
</PropertyDamage>
</Accident>
```

Sample XML File

<Contents>

<Accident>

<Summary>

```

<accident_date>11/19/2003</accident_date>
<accident_time>13:58</accident_time>
<amended> N</amended>
<badge>9999</badge>
<case_number>SS1B13100000</case_number>
<collision_direction>01</collision_direction>
<cost_repair>N</cost_repair>
<county>10</county>
<ctv>1061</ctv>
<day>Wednesday</day>
<first_event>01</first_event>
<formtypeA>MV-104A</formtypeA>
<formversionA>N</formversionA>
<investigated>Y</investigated>
<leftscene>N</leftscene>
<light_conditions>4</light_conditions>
<loc_first_event>1</loc_first_event>
<local_codes>1347509</local_codes>
<ncicori>10901</ncicori>
<nonmotorist_action>77</nonmotorist_action>
<nonmotorist_location>7</nonmotorist_location>
<number_injured>0</number_injured>
<number_killed>0</number_killed>
<number_vehicle>2</number_vehicle>
<officer_first>SAMPLE</officer_first>
<officer_mi>A</officer_mi>
<officer_last>OFFICER</officer_last>
<officer_signature>R0IGODlhFAFBAMQAAAAAAP///wAAAAAAA
  (Actual code representing the signature is in excess of 12 lines;
   it has been abridged here to conserve page space.)
  /Q/DTt61t1bEs/vNL+acJcgAJOhUYIADs=</officer_signature>
<photo>N</photo>
<Rank>TROOPER</Rank>
<reconstructed>N</reconstructed>
<review_date>12/20/2005</review_date>
<review_officer_name>SAMPLE, S Jr</review_officer_name>
<review_officer_signature>R0IGODlhFAFBAMQAAAAAAP///wAAAA
  (Actual code representing the signature is in excess of 12 lines;
   it has been abridged here to conserve page space.)
  OoNuSFz83DHJeEGFUYaZy190YIADs=</review_officer_signature>
<review_time>02:33</review_time>
<road_surface_condition>1</road_surface_condition>

```

<roadway_character>2</roadway_character>
 <station>11</station>
 <traffic_control>02</traffic_control>
 <troop>U</troop>
 <weather_conditions>1</weather_conditions>
 <zone>1</zone>
 <Diagram>R0IGODlhcQL0AcQAAAAAAD/AISChKWipcbDxv8AA
 (Actual code representing the diagram is in excess of 200 lines;
 it has been abridged here to conserve page space.)
 ZWoo4xRo/R0ozeGngoIoQ3AogG7hWOZXCAAOW==</Diagram>
 <XCoordinate>619372</XCoordinate>
 <YCoordinate>4950365</YCoordinate>
 <at_intersection>Y</at_intersection>
 <distance_type></distance_type>
 <intersection>STATE ROUTE 3 (SR)</intersection>
 <reference_marker>3_71081257</reference_marker>
 <road>SMITHFIELD BLVD (TR)</road>
 <narrative>V-1 WAS TRAVELING SOUTH ON SMITHFIELD BLVD.
 V-1 FAILED TO NOTICE THE TRAFFIC LIGHT CHANGE FROM
 GREEN TO RED. V-1 STRUCK V-2 IN THE REAR WHILE V-2 WAS
 STOPPED IN TRAFFIC ON SMITHFIELD BLVD FACING
 SOUTH.</narrative>

</Summary>

<Unit>

<contr_cir_driver>09</contr_cir_driver>
 <contr_cir2_driver>17</contr_cir2_driver>
 <most_damaged_area>02</most_damaged_area>
 <direction_travel>5</direction_travel>
 <hazmat_code>77</hazmat_code>
 <hazmat_released>N</hazmat_released>
 <overdimension_permit>N</overdimension_permit>
 <overweight_permit>N</overweight_permit>
 <point_impact>02</point_impact>
 <total_occupants>02</total_occupants>
 <type_involved>1</type_involved>
 <unit_instance>001</unit_instance>
 <vehicle_long>N</vehicle_long>
 <vehicle_maneuver_action>01</vehicle_maneuver_action>
 <vehicle_towed>N</vehicle_towed>
 <vehicle_wide>N</vehicle_wide>
 <Year>1950</Year>
 <Make>TOYT</Make>
 <VIN>9G1CR32E99C099999</VIN>
 <LicensePlate>ABC1234</LicensePlate>
 <LicenseState>NY</LicenseState>
 <VehRegType>PAS</VehRegType>
 <VehType>4DSD</VehType>
 <Registrant_First_Name>SALLY</Registrant_First_Name>

```

<Registrant_Middle_Name>A</Registrant_Middle_Name>
<Registrant_Last_Name>SAMPLE</Registrant_Last_Name>
<Registrant_Sex>F</Registrant_Sex>
<Registrant_Street_Address_1>1010ANYPLACE
  ST</Registrant_Street_Address_1>
<Registrant_City>YOURCITY</Registrant_City>
<Registrant_State>NY</Registrant_State>
<Registrant_Zip_Code>12121</Registrant_Zip_Code>
<Registrant_Birth_Date>07/18/1983</Registrant_Birth_Date>
<HazMatCardReq>N</HazMatCardReq>
<second_event>77</second_event>
<owner_insurance>888</owner_insurance>
</Unit>
<Unit>
  <contr_cir_driver>77</contr_cir_driver>
  <contr_cir2_driver>77</contr_cir2_driver>
  <most_damaged_area>08</most_damaged_area>
  <direction_travel>5</direction_travel>
  <hazmat_code>77</hazmat_code>
  <hazmat_released>N</hazmat_released>
  <overdimension_permit>N</overdimension_permit>
  <overweight_permit>N</overweight_permit>
  <point_impact>08</point_impact>
  <total_occupants>02</total_occupants>
  <type_involved>1</type_involved>
  <unit_instance>002</unit_instance>
  <vehicle_long>N</vehicle_long>
  <vehicle_maneuver_action>08</vehicle_maneuver_action>
  <vehicle_towed>N</vehicle_towed>
  <vehicle_wide>N</vehicle_wide>
  <Year>1960</Year>
  <Make>CHEV</Make>
  <VIN>9G1ZG99F85F999999</VIN>
  <LicensePlate>ABC9876</LicensePlate>
  <LicenseState>NY</LicenseState>
  <VehRegType>PAS</VehRegType>
  <VehType>4DSD</VehType>
  <Registrant_First_Name>MR</Registrant_First_Name>
  <Registrant_Middle_Name>L</Registrant_Middle_Name>
  <Registrant_Last_Name>SAMPLE</Registrant_Last_Name>
  <Registrant_Sex>M</Registrant_Sex>
  <Registrant_Street_Address_1>2020 ANYTIME
  ST</Registrant_Street_Address_1>
  <Registrant_City>YOURCITY</Registrant_City>
  <Registrant_State>NY</Registrant_State>
  <Registrant_Zip_Code>21212</Registrant_Zip_Code>
  <Registrant_Birth_Date>12/12/1945</Registrant_Birth_Date>

```

```

    <second_event>77</second_event>
    <owner_insurance>888</owner_insurance>
  </Unit>
  <Driver>
    <driver_ejection>1</driver_ejection>
    <driver_safety_system>4</driver_safety_system>
    <driver_seating_position>1</driver_seating_position>
    <unlicensed>N</unlicensed>
    <vio_charge1>1129A</vio_charge1>
    <vio_number1>7B130000SS</vio_number1>
    <First>SALLY</First>
    <Middle>A</Middle>
    <Last>SAMPLE</Last>
    <Street>1010 ANYPLACE ST</Street>
    <City>YOURCITY</City>
    <State>NY</State>
    <ZipCode>12121</ZipCode>
    <DOB>07/18/1983</DOB>
    <Age>27</Age>
    <Gender>F</Gender>
    <LicNumber>00000000</LicNumber>
    <LicState>NY</LicState>
    <InsurCompany>888</InsurCompany>
    <unit_instance>001</unit_instance>
  </Driver>
  <Driver>
    <driver_ejection>1</driver_ejection>
    <driver_safety_system>4</driver_safety_system>
    <driver_seating_position>1</driver_seating_position>
    <unlicensed>N</unlicensed>
    <First>MR</First>
    <Middle>L</Middle>
    <Last>SAMPLE</Last>
    <Street>2020 ANYTIME ST</Street>
    <City>YOURCITY</City>
    <State>NY</State>
    <ZipCode>21212</ZipCode>
    <DOB>12/12/1945</DOB>
    <Age>60</Age>
    <Gender>M</Gender>
    <LicNumber>00000001</LicNumber>
    <LicState>NY</LicState>
    <InsurCompany>888</InsurCompany>
    <unit_instance>002</unit_instance>
  </Driver>
  <Passenger>
    <ejection>1</ejection>
    <safety_equipment>4</safety_equipment>

```

```
<seating_position>03</seating_position>
<unit_no>01</unit_no>
<First>DAUGHTER</First>
<Middle>L</Middle>
<Last>SAMPLE</Last>
<Street>1010 ANYWHERE ST</Street>
<City>YOURCITY</City>
<State>NY</State>
<ZipCode>12121</ZipCode>
<DOB>10/06/1997</DOB>
<Age>18</Age>
<Gender>F</Gender>
</Passenger>
<Passenger>
  <ejection>1</ejection>
  <injured>N</injured>
  <safety_equipment>4</safety_equipment>
  <seating_position>03</seating_position>
  <unit_no>02</unit_no>
  <First>SON</First>
  <Middle>E</Middle>
  <Last>SAMPLE</Last>
  <Street>9999 ANYPLACE RD</Street>
  <City>CITYWHERE</City>
  <State>NY</State>
  <ZipCode>22222</ZipCode>
  <DOB>12/16/1950</DOB>
  <Age>55</Age>
  <Gender>M</Gender>
</Passenger>
</Accident>
</Contents>
```

Accident Report Data Elements

This section contains information on the various data elements captured in the Electronic Accident Reporting System. The table heading definitions are as follows:

NYSP Element—The data element name as per the New York State Police.

Description—What the data element is trying to capture

Optional /Conditional/Required—The level of necessity of the data elements. See the ‘Explanation’ for specifics; this varies depending on what form is being submitted.

Fatal Error—This indicator illustrates fields that must contain a valid value, otherwise the submitted report will be rejected; see ‘Exceptions Handling’ section.

Data Type (Length)—The data format (*numeric, varchar2, date*) allowed in the field, with length limitations.

Explanation—Contains information as to where (what forms) and how the data element is used, and under what conditions.

Note: References to forms MV104AN and MV104W are anticipatory; they are not currently received through the XML/Electronic Accident Reporting system.

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
accident_date	The date the accident occurred.	Required	√	Date (M/D/YYYY)	Required on all Form types.
accident_time	The time of day that the accident took place.	Required	√	Date (HH:MM)	Required on all Form types. Military time.

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
Ammended	Indicates whether the report is an amendment to a previously submitted report (Values: Y - Yes, N - No).	Conditional	√	Varchar2 (1)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
Badge	Badge number of the investigator	Conditional		Varchar2 (5)	Required Forms: MV104S, MV104A, MV104AW, MV104D
case_number	Number assigned to a case entered through the Tracs system.	Required		Numeric (12)	Not a form element
CMV_fatal_injury	NYSP - Number of fatalities associated with the commercial vehicle	Optional		Numeric	Not passed to DMV. Extra element that probably will be removed.
CMV_number_vehic le_person	NYSP - Criteria to determine if an MV-104S will be needed. Specific to TraCS.	Optional		Varchar2 (8)	NYSP Element. Not Passed to DMV- Agencies not using Tracs should not use this element.
CMV_qual_vehicles	NYSP - Criteria to determine if an MV-104S will be needed. Specific to TraCS.	Optional		Varchar2 (6)	NYSP Element. Not Passed to DMV. Agencies not using Tracs should not use this element.
CMV_towed	Total number of vehicles towed from the scene.	Conditional		Numeric	Required Forms: MV104S
CMV_transported	Number of people transported for immediate medical treatment	Conditional		Numeric	Required Forms: MV104S
collision_direction	DMV classification for the manner of collision.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
cost_repair	Indicates whether any vehicles in the accident have more that \$1000 damage.	Conditional		Varchar2 (1)	Required Forms: MV104A, MV104AN
county	County where the accident occurred.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW, MV104S, MV104D
ctv	NYSP - Four digit code of the Municipality	Optional		Numeric	NYSP Element. Not Passed to DMV
day	The day of the week that the accident occurred on. Possible values: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday.	Conditional		Varchar2 (9)	Required Forms: MV104A, MV104AN
fatal_indicator	NYSP - TraCS specific fatal indicator	Optional		CHAR(1)	NYSP Element. Not Passed to DMV
first_event	The first event that occurred during the accident.	Conditional		Numeric (2)	Required on MV104A, MV104AN, MV104AW, MV104S . See Event Type table.

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
formtypeA	Name of the Form Type. This element contains the text MV-104A if the MV-104A form is being sent.	Optional		Varchar2 (7)	This is not a form element; rather it identifies which form(s) the supplied data is associated with.
formtypeD	Name of the Form Type. This element contains the text MV-104D if the MV-104D form is being sent.	Optional		Varchar2 (7)	This is not a form element; rather it identifies which form(s) the supplied data is associated with.
formtypeS	Name of the Form Type. This element contains the text MV-104S if the MV-104S form is being sent.	Optional		Varchar2 (7)	This is not a form element; rather it identifies which form(s) the supplied data is associated with.
formversionA	Version of the Form Type (See Form Types and version Codes).	Optional		Varchar2 (50)	This is not a form element, rather it identifies which form(s) the supplied data is associated with.
formversionD	Version of the Form Type (See Form Types and version Codes).	Optional		Varchar2 (50)	This is not a form element, rather it identifies which form(s) the supplied data is associated with.
formversionS	Version of the Form Type (See Form Types and version Codes).	Optional		Varchar2 (50)	This is not a form element, rather it identifies which form(s) the supplied data is associated with.
investigated	Indicates whether the police investigated the accident (Values: Y - Yes, N - No).	Conditional	√	CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW.
lanes	Number of travel lanes.	Conditional		Numeric (2)	Required Forms: MV104D
leftscene	Indicates whether or not the driver/Individual left the scene of accident (Values: Y - Yes, N - No).	Conditional	√	Varchar 2 (1)	Required Forms: MV104A, MV104AN, MV104AW
light_conditions	Light Condition at time of Accident (see Light Conditions code table)	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
loc_first_event	Indicates whether the vehicles were on-road or off-road (Values: 1-On roadway, 2 - Off roadway, 9 - Unknown).	Conditional	√	Numeric (1)	Required Forms: MV104A, MV104AN, MV104AW
local_codes	Free text field, may be used to enter any identifier a local agency would like to enter.	Optional		Varchar2(30)	Not a form element
ncicori	NCIC Code of the organization reporting the accident.	Conditional	√	Numeric (8)	Required Forms: MV104A, MV104AN, MV104AW, MV104S, MV104D

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
no_buses	Number of buses (with capacity of 9 or more people) involved in the accident	Conditional		Numeric	Required Forms: MV104S
no_hazmat_placard	Number of vehicles with Hazmat Placard involved in the accident.	Conditional		Numeric	Required Forms: MV104S
nonmotorist_action	Action the pedestrian/bicyclist was taking at the time of the accident.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
nonmotorist_location	Location of pedestrian or bicyclist in respect to an intersection at the time of the accident.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
number_injured	Number of people injured in the accident, not including the number killed.	Conditional	√	Numeric	Required Forms: MV104A, MV104AN
number_killed	Number of people killed in the accident	Conditional	√	Numeric	Required Forms: MV104A, MV104AN, MV104D, MV104S, MV104AW
number_vehicle	Number of vehicles involved with the accident.	Conditional	√	Numeric	Required Forms: MV104A, MV104AN, MV104AW
officer_first	First name of the investigator	Conditional		Varchar2 (25)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
officer_mi	Middle name of the investigator	Conditional		Varchar2 (15)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
officer_last	Last name of the investigator	Conditional		Varchar2 (25)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
officer_signature	Investigator's signature (Must be encoded in Base 64 format).	Conditional	√	clob	Required Forms: MV104A, MV104AN, MV104AW, MV104D, MV104S
Original_case_number	NYSP - If an accident is amended, this is the case number from the original accident	Optional		Varchar 2 (18)	NYSP Element. Not Passed to DMV
photo	Indicates whether police took pictures of the accident (Values: Y - Yes, N - No).	Conditional	√	CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
rank	Rank of investigator	Conditional		Varchar2 (20)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
reconstructed	Indicates whether the accident was reconstructed (Values: Y - Yes, N - No).	Conditional	√	CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
reconstructed_shield	Shield number of the officer that did the accident reconstruction	Optional		Varchar 2 (5)	NYSP Element. Not Passed to DMV

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Summary					
review_date	Date of case review by police.	Conditional	√	Date (M/D/YYYY)	Required Forms: MV104AN, MV104A, MV104D, MV104AW
review_officer_name	Reviewing Officer	Conditional		Varchar2 (50)	Required Forms: MV104A, MV104AN, MV104AW
review_officer_signature	NYSP - Signature of reviewing officer (Must be encoded in Base 64 format).	Optional		clob	NYSP Element. Not Passed to DMV
review_time	Time of case review by police.	Conditional		Date (HH:MM)	Required Forms: MV104AN, MV104A, MV104D, MV104AW
road_surface_condition	The condition of the roadway surface at the time of the accident.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
roadway_character	Road characteristics regarding grade and orientation. (See Roadway Character Code table)	Conditional	√	NUMBER (1)	Required Forms: MV104A, MV104AN, MV104AW
roadway_flow	Type of traffic flow at the scene of the accident.	Conditional		Numeric (2)	Required Forms: MV104S
roadway_surface	The type of surface the vehicles were on at the time of the accident.	Conditional		Numeric (2)	Required Forms: MV104D
speed_event	Posted speed limit.	Conditional		Numeric (3)	Required Forms: MV104D
station	Investigator's station, beat, sector	Conditional		Varchar2(5)	Required Forms: MV104S, MV104A, MV104AN, MV104AW, MV104D
traffic_control	Type of traffic control at scene of accident.	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
troop	NYSP - Troop / Division of the Officer	Required		Varchar 2 (2)	Used along with the NYSP element Zone to make up the DMV element Precinct_Post_Troop_Zone; Possible Values: A,B,C,D,E,F,G,H,K,L,M,T,X
truck_sixtires	Number of trucks with 6 or more tires involved in the accident.	Conditional		Numeric	Required Forms: MV104S
tzs	NYSP - Troop, Zone, and Station concatenated together	Optional		Varchar 2 (9)	NYSP Element. Not Passed to DMV
weather_conditions	Weather conditions at the time of the accident	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
work_related	Whether the accident was work related (Values: Y - Yes, N - No).	Conditional		Varchar2 (1)	Required Forms: MV104D
zone	NYSP - Zone / Precinct of the Officer	Required		Varchar 2 (2)	Used along with the NYSP element Troop to

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
					make up the DMV element Precinct_Post_Troop_Zone
Diagram	Diagram of accident (Must be encoded in Base 64 format).	Conditional		clob	Required Forms: MV104A, MV104AN, MV104AW
LocToolVersion	NYSP - Version of the Locator Tool that is used with TraCS	Optional		Varchar 2 (10)	NYSP Element. Not Passed to DMV
CaptureDate	NYSP - Date that the information was captured by Locator Tool	Optional		Date	NYSP Element. Not Passed to DMV
Xcoordinate	Reported latitude of the accident.	Conditional		Numeric (15,4)	Required Forms: MV104A, MV104AN, MV104AW
Ycoordinate	Reported longitude of the accident.	Conditional		Numeric (15,4)	Required Forms: MV104A, MV104AN, MV104AW
Zcoordinate	NYSP - Z Coordinate	Optional		Numeric (15,4)	NYSP Element. Not Passed to DMV
at_intersection	Indicates if the accident occurred within 33 feet of an intersection indicator (Values: Y - Yes, N - No).	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
distance_type	The type of measurement units used to describe distance.	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
intersection	Intersecting Street of the accident.	Conditional		Varchar 2 (30)	Required Forms: MV104A, MV104AN, MV104AW
location_definable	Intersection point of the accident.	Optional		Varchar 2 (30)	Deprecated
literal_description	Intersection point of the accident.	Optional		Varchar 2 (30)	Required forms: MV104A, MV104AN, MV104AW
location_direction	The direction the vehicles were traveling at the time of the accident.	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
location_distance	Distance from reference point or intersection.	Conditional		Numeric (4)	Required Forms: MV104A, MV104AN, MV104AW
loccounty	NYSP - County of accident taken from Locator Tool	Optional		Varchar 2 (25)	NYSP Element. Not Passed to DMV
map_version	NYSP - Version of map used in the locator tool	Optional		Varchar 2 (20)	NYSP Element. Not Passed to DMV
reference_marker	Reference marker point.	Conditional		Varchar2 (12)	Required Forms: MV104A, MV104AN, MV104AW
road	Street on which the accident occurred.	Conditional	√	Varchar 2 (30)	Required Forms: MV104A, MV104AN, MV104AW, MV104D

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Summary					
SnapStatus	NYSP - Snap status in locator tool	Optional		Varchar 2 (2)	NYSP Element. Not Passed to DMV
narrative	Police case notes.	Conditional	√	Varchar2 (2000)	Required Forms: MV104S, MV104A, MV104AN, MV104AW

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Unit					
access_control	Type of road access.	Conditional		Numeric (2)	Required Forms: MV104S
cargo_body	Vehicle Cargo Body Type	Conditional		Numeric (2)	vehicle configuration must be bus if cargo body type is bus (vehicle configuration is Single-unit truck: 2 axles, 6 tires and cargo type is Bus (Seats 9 - 15 people including driver)) Required Forms: MV104S
carrier_explanation	NYSP - Further explanation of the events of the CMV accident	Optional		Varchar 2 (55)	NYSP Element. Not Passed to DMV
Carrier_Source	Carrier Source – (To be depreciated-tentative date 6/06)	Conditional		Varchar2 (1)	Required Forms: MV104S
CMV_first_event	Supplemental Event	Conditional		Numeric(2)	Required Forms: MV104S
CMV_second_event	Supplemental Event	Conditional		Numeric(2)	Required Forms: MV104S
CMV_third_event	Supplemental Event	Conditional		Numeric(2)	Required Forms: MV104S
CMV_fourth_event	Supplemental Event	Conditional		Numeric(2)	Required Forms: MV104S
Comm_Vehicle_Type	Truck Bus Class code of commercial vehicle (see Truck Bus Class code table)	Conditional		Varchar 2 (2)	IF the vehicle is a truck it must have an acceptable truck class and a body type of one of the following: SUBURBAN ,UNKNOWN TRUCK, TRACTOR, DELIVERY TRUCK, DUMP, FLAT BED TRUCK, STAKE TRUCK, TANK TRUCK, REFRIGERATOR TRUCK, TOW TRUCK, VAN TRUCK, UTILITY, POLE TRAILER,SEMI-TRAILER, TRAILER

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Unit					
					If the vehicle is a bus it must have a vehicle class of Transit bus or over the road coach and it must have a body type of SUBURBAN or BUS (OMNIBUS)
					Acceptable Truck bus classes are 'C1','C2','C3','D1','D2','D3','E1','E2','E3','F1','F2','F3','G1','G2','G3','H1','H2','H3','I1','I2','I3','J1','J2','J3','K1','K2','K3','L1','L2','L3','M1','M2','M3' see list for truck bus class codes
					Required Forms: MV104A, MV104AN, MV104AW
contr_cir_driver	Primary contributing factor	Conditional	√	NUMBER (2)	Required Forms: MV104A, MV104AN, MV104AW
contr_cir2_driver	Secondary contributing factor	Conditional		NUMBER (2)	Required Forms: MV104A, MV104AN, MV104AW
most_damaged_area	Type of Damage to the vehicle	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
damaged_area	Category of Damage to the vehicle.	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
direction_travel	Direction the vehicle was traveling at the time of the accident.	Conditional	√	Varchar 2 (2)	Direction of vehicle must be entered if Body Type is entered Direction of Travel cannot be null Required Forms: MV104A, MV104AN, MV104AW
estimated_speed	Speed of travel	Conditional		Numeric (3)	Required Forms: MV104D
gross_weight	Vehicle gross weight in pounds	Conditional		Numeric (6)	Must be a numeric Value Required Forms: MV104S
hazmat_class_name	Name of hazardous materials class. This is a free text field.	Conditional		Varchar2 (25)	Required Forms: MV104S
hazmat_code	Standard Hazardous material code	Conditional		Numeric (4)	Required Forms: MV104S, MV104A, MV104AN, MV104AW
hazmat_placard_info	Type of Hazardous Material Placard	Conditional		Numeric (3)	Required Forms: MV104S, MV104A, MV104AN, MV104AW
hazmat_released	Indicates whether hazardous material was released from a vehicle. Possible values Y-	Required		Char (1)	Required Forms: MV104A, MV104S

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Unit					
	Yes or N- No.				
hazmat_type	Detailed Type of Hazardous Material	Conditional		Numeric (5)	Required Forms: MV104S, MV104A, MV104AN, MV104AW
no_axles	Total number of axles, including trailer	Conditional		Numeric (2)	Required Forms: MV104S
overdimension_permit	Over-dimension permit indicator (Values: Y - Yes, N - No).	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
overweight_permit	Overweight permit indicator (Values: Y - Yes, N - No).	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
point_impact	Category of Damage to the vehicle.	Conditional		NUMBER (2)	Required Forms: MV104A, MV104AN, MV104AW
total_gross_weight	Total gross weight of all trailers in pounds.	Conditional		Numeric	Required Forms: MV104S
total_occupants	The number of passengers in the vehicle at the time of the accident, including the driver. Must be in two digit format, e.g. '01', or '04.'	Conditional		Numeric (2)	Number of occupants is required if vehicle plate# and body type information is supplied Must be numeric, unknown or not applicable Required Forms: MV104A, MV104AN, MV104AW
type_involved	Identifies the type of vehicle involved. (Values: 1 – vehicle, B – bicyclist, P – pedestrian, A – all terrain, S – snowmobile, I – inline skater, O – other.)	Conditional	√	Varchar2 (1)	See Vehicle ID table; Bicyclist (operator) or Other Pedestrian must be used if the safety equipment used was: In-line skates bicyclist (Helmet Only), In-line Skates Bicyclist (Helmet/Other), In-line skates Bicyclist (Pads Only), and In-line Skates Bicyclist (Stoppers Only) Required Forms: MV104A, MV104AN, MV104AW
unit_instance	Identifies the order of Vehicles in the accident, unique for a Case	Required	√	Numeric (3)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
unknown_speed	Indicates whether the speed of the vehicle was known at the time of the accident (Values: Y - Yes, N - No).	Conditional		Char (1)	Required Forms: MV104D
vehicle_configuration	Configuration of the vehicle	Conditional		Numeric (2)	vehicle configuration must be bus if cargo body type is bus (vehicle configuration is Single-unit truck: 2 axles, 6 tires and cargo type is Bus (Seats 9 - 15 people including driver))

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Unit					
					Required Forms: MV104S
vehicle_long	More than 34 feet long indicator (Values: Y - Yes, N - No).	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
vehicle_maneuver_action	Action of the vehicle prior to the accident. (See Vehicle Maneuver code table for possible values)	Conditional	√	Numeric (2)	Pre-accident action cannot be null Required Forms: MV104A, MV104AN, MV104AW
vehicle_towed_by	Describes who the vehicle was towed by	Conditional		Varchar2 (14)	Required Forms: MV104A, MV104AN, MV104AW
vehicle_towed_to	Describes where the vehicle was towed.	Conditional		Varchar2 (14)	Required Forms: MV104A, MV104AN, MV104AW
vehicle_towed	Indicates if vehicle was towed from scene (Values: Y - Yes, N - No).	Optional		CHAR (1)	Should be supplied with the Forms: MV104A MV104AN, MV104AW
vehicle_wide	More than 95 inches wide indicator (Values: Y - Yes, N - No).	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN, MV104AW
Year	Four digit model year for which the vehicle was manufactured	Conditional		Numeric (4)	This must be a numeric value e.g. 2005 Required Forms: MV104A, MV104AW, MV104AN
Make	Make of the vehicle (See Vehicle Make table for possible values)	Conditional		Varchar2 (5)	Required Forms: MV104A, MV104AN, MV104AW
Model	FARS classification of the vehicle model. (See Vehicle Model for possible values)	Conditional		Varchar2 (4)	Required Forms: MV104D
Vin	Vehicle Identification Number	Conditional		Varchar2 (17)	Required Forms: MV104A, MV104AN, MV104AW, MV104S
LicensePlate	A Vehicle's plate number.	Conditional		Varchar2 (10)	Length of plate number must not exceed 8 characters if vehicle is registered in NY state Plate number is required if vehicle is registered in NY state and body type is known Plate number or Body type must be entered if Public Property Damage information is supplied Required Forms: MV104A, MV104AN, MV104AW, MV104S
LicenseState	State code where auto is registered	Conditional		Varchar2 (2)	Required Forms: MV104A, MV104AN, MV104AW, MV104S
HazMatPlate	NYSP - Four digit Placard Number. This	Conditional		Varchar2 (4)	Required Forms: MV104S

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Unit					
	comes from the middle of the diamond or from the rectangular box and the one digit number from the bottom of the diamond.				
VehRegType	The registration class the vehicle belongs to. See Registration Class table.	Optional		Varchar2 (3)	Required for all registered vehicles in NYS. Not currently Passed to DMV; <u>will</u> be used in the future.
VehType	Vehicle body type (See table for possible values)	Conditional		Varchar2 (4)	Body Type is required when plate number has been provided Body Type is required for any vehicle Plate number or Body type must be entered if Public Property Damage information is supplied Required Forms: MV104A, MV104AN, MV104AW
CarrierName	The carrier's name.	Conditional		Varchar2 (100)	Required Forms: MV104S
CarrierStreet	The carrier's street address line 1	Conditional		Varchar2 (30)	Required Forms: MV104S
CarrierCity	The carrier's address city	Conditional		Varchar2 (25)	Required Forms: MV104S
CarrierState	The carrier's address state code	Conditional		Varchar2 (2)	Required Forms: MV104S
CarrierZipCode	The carrier source address zip code	Conditional		Varchar2 (9)	Required Forms: MV104S
CarrierDOTNumber	DOT ID Number	Conditional		Varchar2 (20)	Required Forms: MV104S
CarrierICCNNumber	ICC MC ID Number	Conditional		Varchar2 (6)	Required Forms: MV104S
Registrant_First_Name	First name of the individual the vehicle is registered to.	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_Middle_Name	Middle name of the individual the vehicle is registered to.	Conditional		Varchar2 (15)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_Last_Name	Last name of the individual the vehicle is registered to.	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_Sex	The gender of the registrant	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_Street_Address_1	Registrant street address line 1	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_City	Registrant city	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_State	Registrant address state code	Conditional		Varchar2 (2)	Required Forms: MV104A, MV104AN,

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Unit					
					MV104AW
Registrant_Zip_Code	Registrant address zip code.	Conditional		Varchar2 (9)	Required Forms: MV104A, MV104AN, MV104AW
Registrant_Birth_Date	Registrant Date of Birth (for individuals only)	Conditional		Date (M/D/YYYY)	Required Forms: MV104A, MV104AN, MV104AW
HazMatCardReq	Hazardous Material Placard indicator (Values: Y - Yes, N - No).	Conditional		Varchar2 (1)	Required Forms: MV104S
second_event	Code with the second vehicle event (See Event types table for possible values)	Optional	√	Numeric (2),	Required forms: MV104A, MV104AN, MV104AW
owner_insurance	Insurance Carrier Code	Conditional		Varchar2 (3)	Required Forms: MV104A, MV104AN, MV104AW

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
driver_airbag_not_vehicle	Indicates whether airbags were in the vehicle at the time of the accident. (Values: Y - Yes, N - No).	Conditional		CHAR (1)	Required Forms: MV104D
driver_airbags_deployed	Indicates whether airbags were deployed. (Values: Y - Yes, N - No).	Conditional		CHAR (1)	Required Forms: MV104D
driver_condition	Emotional state of individual at scene of accident.	Conditional	√	Numeric (1)	Driver_condition should be entered for a Police report when a driver_type_complaint is entered When injury information is entered for an individual, then the driver_type_complaint, Driver_condition and injury location cannot have a value of not applicable

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
					Driver_loc_complaint and Driver_type_complaint should be entered when Driver_condition is entered for a Police Reported injury. Required Forms: MV104A, MV104AN, MV104AW
CMV_Driver_condition	Condition of the driver at the time of the accident	Conditional		Numeric (2)	Required Forms: MV104S
driver_date_death	Date of individual's death.	Conditional		Date (M/D/YYYY)	Date of Death must be date of accident or later. Required Forms: MV104A, MV104AN, MV104AW
driver_time_death	Military time of individual's death.	Conditional		Date (HH:MM)	Required Forms: MV104D
driver_deceased	Indicates if individual is deceased. (Values: Y - Yes, N - No).	Conditional		Char (1)	Required Forms: MV104D
driver_ejection	Type of ejection from the vehicle.	Conditional	√	Numeric (2)	Must have a value if the accident involves a fatality, an injury, or property damage and injury. If the accident does not involve a fatality and an driver_ejection is provided, then the following information must also be supplied: sex, seat position, and age. Required Forms: MV104A, MV104AN, MV104AW
driver_injured	NYSP - Injured flag specific to TraCS	Optional		Char (1)	NYSP Element. Not Passed to DMV. Agencies not using Tracs should not use this element.
driver_loc_complaint	Location of individual's injury	Conditional		Numeric (2)	When the driver_loc_complaint is provided for the driver then driver_safety_system, age, sex, seat position and ejection type must be specified (required for an injured individual)

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
					An injury must be associated with an driver_loc_type Driver_Condition and driver_loc_complaint should be entered when an injury is entered for a Police Reported injury. Required Forms: MV104A, MV104AN, MV104AW
driver_Med_Facility	The location where the injured individual was taken. (See the medical facility table for possible values.)	Conditional		Numeric (4)	An individual taken by an ambulance or other emergency vehicle must be taken somewhere. If the driver_source_transport information is provided then the Med_Facility information must be provided as well. Required Forms: MV104A, MV104AN, MV104AW
hospital_information_name	The name of the hospital that the individual was taken to.	Conditional		Varchar2 (30)	Required Forms: MV104D
hospital_information_county	The county of the hospital where the individual was taken to.	Conditional		Varchar2 (10)	Required Forms: MV104D
hospital_information_state	The state of the hospital that the individual was taken to.	Conditional		Varchar2 (2)	Required Forms: MV104D
driver_other_hospital	Out of state hospital name	Optional		Varchar2 (30)	Required Forms: MV104D
driver_other_hospital_county	Out of state hospital county	Optional		Varchar2 (10)	Required Forms: MV104D
driver_other_hospital_state	Out of state hospital state	Optional		Varchar2 (2)	Required Forms: MV104D
driver_med_notified	Time of Emergency Medical Service Notification	Conditional		Date (HH:MM)	Required Forms: MV104D
driver_med_arrived	Time Emergency Medical Service Arrived	Conditional		Date (HH:MM)	Required Forms: MV104D
driver_med_arrived_hospital	Time Emergency Medical Service Arrived at hospital	Conditional		Date (HH:MM)	Required Forms: MV104D
driver_owner_known	NYSP - TraCS specific field describing the vehicle/driver	Optional		Char(1)	NYSP Element. Not Passed to DMV

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
driver_safety_system	Type of safety equipment used by the individual.	Conditional	√	Numeric (2)	<p>A driver_safety_system of helmet (6) can only be used for a driver or passenger of a motorcycle.</p> <p>Must have a value if the accident involves a fatality, an injury, or property damage and injury.</p> <p>Required Forms: MV104A, MV104AN, MV104AW</p>
driver_seating_position	Seat Position of Individual	Conditional	√	Numeric (2)	<p>Must be (1) for driver</p> <p>There can only be one driver per vehicle</p> <p>Must have a value if the accident involves a fatality, an injury, or property damage and injury.</p> <p>If the accident does not involve a fatality and a driver_seating_position is provided then the following information must also be supplied: sex, ejection type, and age.</p> <p>Only Drivers and Registrants can have a seat position of driver (1).</p>

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
					Required Forms: MV104A, MV104AN, MV104AW
driver_source_transport	Type of vehicle that took the individual to the hospital. (Possible values: See the source transport table).	Conditional		Varchar2 (4)	An individual taken by an ambulance or other emergency vehicle must be taken somewhere. If the driver_source_transport information is provided then the Med_Facility information must be provided as well. Required Forms: MV104A, MV104AN, MV104AW
driver_type_complaint	Type of injury sustained by the individual.	Conditional		Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW
extricated	Indicates if extrication was used to remove the individual from the vehicle (Values: Y - Yes, N - No).	Conditional		Varchar2 (1)	Required Forms: MV104D
extrication_equipment	Type of extrication equipment used to remove the individual from the vehicle; this is a free text field.	Conditional		Varchar2 (20)	Required Forms: MV104D
unlicensed	Indicates whether the driver is licensed (Values: Y - Yes, N - No).	Conditional		CHAR (1)	When the driver's license state is not specified and there is no license record for this driver, then the Unlicensed driver Indicator must be set to a 'Y'. Required Forms: MV104A, MV104AN, MV104AW
vio_charge1	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW
vio_charge2	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW
vio_charge3	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW
vio_charge4	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW
vio_charge5	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW

Electronic Ticket/Accident Reporting Specifications

NYSP Element	Description	Optional/ Conditional/ Required	Fatal Error	Data Type (Length)	Explanation
Driver					
vio_charge6	Ticket violation Code (See Violation Codes chart for possible values)	Conditional		Varchar2 (8)	Required Forms: MV104A, MV104AN, MV104AW
vio_number1	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
vio_number2	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
vio_number3	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
vio_number4	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
vio_number5	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
vio_number6	Ticket Number	Conditional		Varchar2 (10)	Required Forms: MV104A, MV104AN, MV104AW
First	The first name of individual involved in accident.	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
Middle	The middle name of individual involved in accident.	Required		Varchar2 (15)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
Last	The last name of individual involved in accident.	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
Street	Street address line 1	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
City	Individual's address city.	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
State	Address state code	Required		Varchar2 (2)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
ZipCode	Address zip code	Required		Varchar2 (9)	Required Forms: MV104A, 104AN, 104AW, 104S, 104D (All Forms)
DOB	Individual's date of birth.	Conditional		Date (M/D/YYYY)	Must be supplied if age is supplied Required Forms: MV104AN, MV104S, MV104A, MV104AW
Age	Individual's age at the time of the accident.	Conditional	√	Numeric (3)	Must have a value if the accident involves a fatality, an injury, or property damage and injury.

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
					When the Date of birth of the driver is entered, the Age cannot be null or unknown for the Driver of the Vehicle
					If the accident does not involve a fatality and individual age is provided then the following information must also be supplied: sex, ejection type, and seat position.
					Required Forms: MV104A, MV104AN, MV104AW
Gender	The sex of the individual. (M=male; F=female; X=unknown)	Conditional	√	Varchar2 (1)	Must have a value if the accident involves a fatality, an injury, or property damage and injury.
					If the accident does not involve a fatality and individual sex is provided then the following information must also be supplied: age, ejection type, seat position.
					Required Forms: MV104A, MV104AN, MV104AW
LicNumber	Driver License Number	Conditional		Varchar2 (25)	Required Forms: MV104A, MV104AN, MV104AW, MV104S
LicType	NYSP - Class of driver license	Optional		Varchar2 (9)	NYSP Element. Not Passed to DMV currently; DMV will use this element in a future release (June).
LicState	State code from which the driver license was obtained	Conditional		Varchar2 (2)	License state must be entered if role type is driver or license number is entered
					When the driver's license state is not specified then the Unlicensed driver Indicator must be set to a Y
					Required Forms: MV104AN MV104A, MV104AW
InsurCompany	Driver insurance carrier name; see Insurance Company Codes table	Conditional		Numeric (3)	Required forms: MV104A, MV104AN, MV104AW

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Driver					
unit_instance	Identifies the order of Vehicles in the accident, unique for a Case	Conditional	√	Number (3)	Required Forms: MV104A, MV104AN, MV104AW

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
airbags_deployed	Indicates whether airbags were deployed. (Values: Y - Yes, N - No).	Conditional		CHAR (1)	Required Forms: MV104D
airbags_not_vehicle	Indicates whether airbags were in the vehicle at the time of the accident. (Values: Y - Yes, N - No).	Conditional		CHAR (1)	Required Forms: MV104D
date_death	Date of individual's death.	Conditional		Date (M/D/YYYY)	Date of Death must be date of accident or later. Required Forms: MV104A , MV104AN, MV104AW,
deceased	Indicates if individual is deceased. (Values: Y - Yes, N - No).	Conditional		Char (1)	Required Forms: MV104D
ejection	Type of ejection from the vehicle.	Conditional		Numeric (2)	Must have a value if the accident involves a fatality, an injury, or property damage and injury. If the accident does not involve a fatality and individual ejection type is provided then the following information must also be supplied: sex, seat position, and age. Required Forms: MV104A, MV104AN, MV104AW
extricated	Indicates if extrication was used to remove the individual from the vehicle (Values: Y - Yes, N - No).	Conditional		Varchar2 (1)	Required Forms: MV104D
extrication_type	Type of extrication equipment used to	Conditional		Varchar2 (20)	Required Forms: MV104D

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
	remove the individual from the vehicle; This is a free text field.				
injured	NYSP - Injured flag specific to TraCS	Optional		Char (1)	NYSP Element. Not Passed to DMV. Agencies not using Tracs should not use this element.
loc_complaint	Location of individual's injury	Conditional	√	Numeric (2)	When the loc_complaint is provided for a passenger then the safety_equipment, age, sex, seating_position and ejection must be specified(required for an injured individual) Person_condition and type_complaint should be entered when loc_complaint is entered for a Police Reported injury. A type_complaint must be associated with an injury location Required Forms: MV104A, MV104AN, MV104AW Required Forms: MV104D
med_arrived	Time Emergency Medical Service Arrived	Conditional		Date (HH:MM)	Required Forms: MV104D
med_arrived_hospital	Time Emergency Medical Service Arrived at hospital	Conditional		Date (HH:MM)	An individual taken by an ambulance or other emergency vehicle must be taken somewhere. If the driver_source_transport information is provided then the med_facility information must be provided as well.
hospital_information_name	The name of the hospital that the individual was taken to.	Conditional		Varchar2 (30)	Required Forms: MV104D
hospital_information_county	The county of the hospital where the individual was taken to.	Conditional		Varchar2 (10)	Required Forms: MV104D
hospital_information_state	The state of the hospital that the individual was taken to.	Conditional		Varchar2 (2)	Required Forms: MV104D
med_facility	The location where the injured individual was taken. (See Medical Facility code table.)	Conditional		Numeric (4)	Required Forms: MV104A, MV104AN Required Forms: MV104D
med_notified	Time of Emergency Medical Service	Conditional		Date (HH:MM)	Required Forms: MV104D

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
	Notification				
other_hospital	Out of state hospital name	Conditional		Varchar2 (30)	Required Forms: MV104D.
other_hospital_co	Out of state hospital county	Optional		Varchar2 (10)	Required Forms: MV104D
other_hospital_state	Out of state hospital state	Optional		Varchar2 (2)	Required Forms: MV104D
person_condition	Emotional status of individual at scene of accident.	Conditional		Numeric (1)	When injury information is entered for an individual, then the type_complaint, person_condition and loc_complaint cannot have a value of not applicable
					Loc_complaint and type_complaint should be entered when person_condition is entered for a Police Reported injury.
					Required Forms: MV104A, MV104AN, MV104AW
safety_equipment	Type of safety equipment used by the individual.	Conditional	√	Numeric (2)	For the safety_equipment: In-line Skates Bicyclist(Helmet Only), In-line Skates Bicyclist(Helmet/Other), In-line Skates Bicyclist(Pads Only), In-line Skates Bicyclist(Stoppers Only) the unit's type_involved must be Bicyclist (operator),or Other Pedestrians (e.g. occupants of transport device used as equipment, occupant in a building),
					Safety_equipment cannot be null or (-) not applicable when, the individual's seat position is bicyclist.
					A type_involved of Bicyclist (operator) or Other Pedestrian must be used if the safety_equipment used was: In-line skates bicyclist (Helmet Only), In-line Skates Bicyclist (Helmet/Other), In-line skates Bicyclist (Pads Only), and In-line Skates Bicyclist (Stoppers Only)

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
					<p>Must have a value if the accident involves a fatality, an injury, or property damage and injury.</p> <p>Required Forms: MV104A, MV104AN, MV104AW</p>
seating_position	Seat Position of Individual	Conditional	√	Numeric (2)	<p>Must be (4) for bicyclist</p> <p>Type_involved's that are not vehicle based must have a seating_position of "-"(not applicable). Non-Vehicle based role types include: registrant of unoccupied vehicle, pedestrian; other pedestrians (occupants of transport device used as equipment, occupant in a building) skateboarder.</p> <p>Must have a value if the accident involves a fatality, an injury, or property damage and injury.</p> <p>If the accident does not involve a fatality and seating_position is provided then the following information must also be supplied: sex, ejection type, age.</p> <p>For the type_involved of bicyclist the seating position cannot be null or (-) not applicable</p> <p>Registrants can have a seating position of 1 (Driver)</p> <p>If individual is a bicyclist then seating position and safety_equipment information must be entered</p> <p>Required Forms: MV104A, MV104AN, MV104AW</p>

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
					An individual taken by an ambulance or other emergency vehicle must be taken somewhere. If the source_transport information is provided then the med_facility information must be provided as well.
source_transport	The manner in which an injured individual was transported; from the table 'source_transport'; if no codes apply, license plate number may be entered.	Conditional		Varchar2 (8)	Required Forms: MV104D, MV104A, MV104AN, MV104AW Required Forms: MV104D
time_death	Military time of individual's death.	Conditional		Date (HH;MM)	Required Forms: MV104A, MV104AN, MV104AW
type_complaint	Type of injury sustained by the individual.	Conditional	√	Numeric (2)	Individual vehicle ID's of Bicyclist (operator) or Other Pedestrian must be used if the safety equipment used was: In-line skates bicyclist(Helmet Only), In-line Skates Bicyclist(Helmet/Other), In-line skates Bicyclist (Pads Only), and In-line Skates Bicyclist(Stoppers Only)
unit_no	The vehicle the passenger was traveling in.	Conditional	√	Numeric (2)	Required Forms: MV104A, MV104AN, MV104AW Required Forms: MV104A, 104AN, 104AW, 104D
First	The first name of individual involved in accident.	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104D
Middle	The middle name of individual involved in accident.	Required		Varchar2 (15)	Required Forms: MV104A, 104AN, 104AW, 104D
Last	The last name of individual involved in accident.	Required		Varchar2 (25)	Required Forms: MV104A, 104AN, 104AW, 104D
Street	Street address line 1	Required		Varchar2 (25)	Required Forms: MV104D
City	Individual's address city.	Required		Varchar2 (25)	Required Forms MV104D
State	Address state code	Required		Varchar2 (2)	Required Forms: MV104D
ZipCode	Address zip code	Required		Varchar2 (9)	Required Forms: MV104D
DOB	Individual's date of birth.	Optional		Date (M/D/YYYY)	Must be supplied if age is supplied Required Forms: MV104D

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Passenger					
					Should have a value if the accident involves a fatality, an injury, or property damage and injury.
Age	Individual's age at the time of the accident.	Conditional	√	Numeric (3)	If the accident involves a fatality and the age is provided then the following information must be supplied: sex, ejection_type, and seating_position. Required Forms: MV104A, MV104AN, MV104AW Must have a value if the accident involves a fatality, an injury, or property damage and injury.
Gender	The sex of the individual. (m=male; f=female; x=unknown)	Conditional	√	Varchar2 (1)	If the accident does not involve a fatality and individual sex is provided then the following information must also be supplied: age, ejection type, seat position.

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error s</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Property Damage					
OwnerFirstName	NYSP - Owner's first name	Optional		Varchar2 (25)	NYSP Element. Not Passed to DMV. We collect all this information and then add it on to the Narrative before it is transferred.
OwnerMiddleInitial	NYSP - Owners' middle initial	Optional		Varchar2 (1)	
OwnerLastName	NYSP - Owner's last name	Optional		Varchar2 (25)	
OwnerStreetAddress	NYSP - Owner's address	Optional		Varchar2 (25)	
OwnerCity	NYSP - Owner's city	Optional		Varchar2 (25)	
OwnerState	NYSP - Owner's state	Optional		Varchar2 (2)	

Electronic Ticket/Accident Reporting Specifications

<i>NYSP Element</i>	<i>Description</i>	<i>Optional/ Conditional/ Required</i>	<i>Fatal Error s</i>	<i>Data Type (Length)</i>	<i>Explanation</i>
Property Damage					
OwnerZip	NYSP - Owner's zip code	Optional		Varchar2 (9)	
Unit_Instance	NYSP - Unit number that was associated with the property damage	Optional	√	Numeric (2)	
object_damaged	Description of the public property damage.	Conditional		Varchar2 (30)	Required Forms: MV104A, MV104AN
owner_notified	NYSP - Was the owner notified (Values: Y - Yes, N - No)	Optional		CHAR(1)	NYSP Element. Not Passed to DMV
PrivatePropertyDamaged	Indicates whether the vehicle caused private property damage. (Values: Y - Yes, N - No)	Conditional		CHAR(1)	Required Forms: MV104A, MV104AN MV104W
PublicPropertyDamage	Indicates whether the vehicle caused public property damage. (Values: Y - Yes, N - No)	Conditional	√	CHAR(1)	Required Forms: MV104A, MV104AN MV104W

Exceptions Handling

DMV staff through an Exceptions Handling Process will deal with some errors that are encountered in order to get as many tickets on to the file as possible without excessive communications back and forth with the sending agency. However, certain errors designated as fatal errors will be returned to the State Police who will post them on an informational web site (the State Police will send the URL, along with other information, once a signed TraCS User Agreement is returned to them.) State Police will not return an acknowledgement to the sending agency, so the agency will need to regularly check the website in order to view any problems that are encountered. If DMV finds that there are excessive non-fatal errors of a particular type, it will communicate that information to the sending agency. If the type of error is not corrected in subsequent transmissions, DMV will either tag the errors as fatal and return them, or discontinue the agency's ability to send electronic information.

Some of the errors listed are "file level" errors, some are "transaction level" errors, and still others can apply to either a batch file or an individual transaction depending on where in the XML file the <MESSAGE_TEXT> element occurs:

- The error is a file level error if the message occurs within the "outer" XML of the batch file. You will need to correct the problem and resubmit the entire input file.
- The error is a transaction level error if the message occurs in the "inner" XML that is contained within the <TRANSACTIONS> node of the batch file. Depending on the specific error, you may be able to correct the problem and resubmit the transaction as part of another input batch.
- Do not resubmit the whole batch to correct a transaction error

You should always refer to the State Police web site to determine if you can correct the problem yourself before requesting DMV support. Then, if it becomes necessary to contact DMV for assistance, you will need to provide all of the following information:

- 1) the complete file name of the XML file in which the error was returned;
- 2) the exact error code and message text returned; and
- 3) the identifying input data, (Ticket #, Client Id, Plate # etc) if the error is a transaction error.

All requests for DMV support should be coordinated through your organization's designated liaison.

New York Driving License 2D Barcode Format

There are three different formats of 2D PDF417 barcodes on New York Driving Licenses.

- Licenses issued prior to September 15th 2005
- Licenses Issued between September 15th 2005 and October 21st 2005
- Licenses Issued after October 21st 2005
- Licenses Issued after January 11th 2006

Licenses issued prior to September 15th 2005

Length 276 Bytes.

Field	Length	Byte Position	Value
Start Character	1	1	'@'
Line Feed	1	2	0x0A
Record Separator	1	3	0x1C
Carriage Return	1	4	0x0D
File Type	5	5-9	"AAMVA"
Jurisdiction Code	5	10-14	"36001"
Version Number	1	15	"0"
Sub Files	2	16-17	"01"
Sub File Header	10	18-27	"DL00270249"
Sub File ID	2	28-29	"DL"
Line Feed	1	30	0x0A
Name Header	3	31-33	"DAA"
Name Field	35	34-68	Name Field with commas translated to '@'
Line Feed	1	69	0x0A
Street Header	3	70-72	"DAG"
Street Field	20	73-92	Address Street Information
Line Feed	1	93	0x0A
City Header	3	94-96	"DAI"
City Field	15	97-111	Address City Information
Line Feed	1	112	0x0A
State Header	3	113-115	"DAJ"
State Field	2	116-118	"NY"
Line Feed	1	119	0x0A
Zip Code Header	3	120-122	"DAK"
Zip Code Field	11	123-132	Address Zip Code Information
Line Feed	1	133	0x0A
License Number Header	3	134-136	"DAQ"
License Number Field	25	137-161	License Number
Line Feed	1	162	0x0A

Electronic Ticket/Accident Reporting Specifications

Field	Length	Byte Position	Value
Date of Birth Header	3	163-165	“DBB”
Date of Birth Field	8	166-173	Date of birth in the format yyyymmdd
Line Feed	1	174	0x0A
Date of Issue Header	3	175-177	“DBD”
Date of Issue Field	8	178-185	Date of issue in the format yyyymmdd
Line Feed	1	186	0x0A
Date of Expiry Header	3	187-189	“DBA”
Date of Expiry Field	8	190-197	Date of Expiry in the format yyyymmdd
Line Feed	1	198	0x0A
Document Class Header	3	199-201	“DAR”
Document Class Field	4	202-205	Document Class
Line Feed	1	206	0x0A
Restriction Header	3	207-209	“DAS”
Restriction Field	10	210-219	Restrictions
Line Feed	1	220	0x0A
Endorsement Header	3	221-223	“DAT”
Endorsement Field	6	224-229	Endorsements
Line Feed	1	230	0x0A
Gender Header	3	231-333	“DBC”
Gender Field	1	234	Gender Code. 0 = Unknown, 1 = Male, 2 = Female, 9 = Other.
Line Feed	1	235	0x0A
Height Header	3	236-238	“DAU”
Height Field	3	239-241	Height in format FeetInches e.g. 511
Line Feed	1	242	0x0A
Eye Color Header	3	243-245	“DAY”
Eye Color Field	3	246-248	Eye color
Line Feed	1	249	0x0A
Social Number Header	3	250-252	“DBK”
Social Number Field	9	253-261	BLANK
Line Feed	1	262	0x0A
Organ Donor Header	3	263-265	“DBH”
Organ Donor Field	10	266-275	Organ Donor
Carriage Return	1	276	0x0D

Licenses Issued between September 15th 2005 and October 21st 2005

Length 276 Bytes.

Changes to the previous version:

- Endorsement field extended from 6 characters to 8 characters
- Donor field reduced to 9 characters
- Missing Carriage Return character from the end of the barcode

Field	Length	Byte Position	Value
Start Character	1	1	'@'
Line Feed	1	2	0x0A
Record Separator	1	3	0x1C
Carriage Return	1	4	0x0D
File Type	5	5-9	"AAMVA"
Jurisdiction Code	5	10-14	"36001"
Version Number	1	15	"0"
Sub Files	2	16-17	"01"
Sub File Header	10	18-27	"DL00270249"
Sub File ID	2	28-29	"DL"
Line Feed	1	30	0x0A
Name Header	3	31-33	"DAA"
Name Field	35	34-68	Name Field with commas translated to '@'
Line Feed	1	69	0x0A
Street Header	3	70-72	"DAG"
Street Field	20	73-92	Address Street Information
Line Feed	1	93	0x0A
City Header	3	94-96	"DAI"
City Field	15	97-111	Address City Information
Line Feed	1	112	0x0A
State Header	3	113-115	"DAJ"
State Field	2	116-118	"NY"
Line Feed	1	119	0x0A
Zip Code Header	3	120-122	"DAK"
Zip Code Field	11	123-132	Address Zip Code Information
Line Feed	1	133	0x0A
License Number Header	3	134-136	"DAQ"
License Number Field	25	137-161	License Number
Line Feed	1	162	0x0A
Date of Birth Header	3	163-165	"DBB"
Date of Birth Field	8	166-173	Date of birth in the format yyyymmdd
Line Feed	1	174	0x0A

Electronic Ticket/Accident Reporting Specifications

Field	Length	Byte Position	Value
Date of Issue Header	3	175-177	“DBD”
Date of Issue Field	8	178-185	Date of issue in the format yyyymmdd
Line Feed	1	186	0x0A
Date of Expiry Header	3	187-189	“DBA”
Date of Expiry Field	8	190-197	Date of Expiry in the format yyyymmdd
Line Feed	1	198	0x0A
Document Class Header	3	199-201	“DAR”
Document Class Field	4	202-205	Document Class
Line Feed	1	206	0x0A
Restriction Header	3	207-209	“DAS”
Restriction Field	10	210-219	Restrictions
Line Feed	1	220	0x0A
Endorsement Header	3	221-223	“DAT”
Endorsement Field	8	224-231	Endorsements
Line Feed	1	232	0x0A
Gender Header	3	233-335	“DBC”
Gender Field	1	236	Gender Code. 0 = Unknown, 1 = Male, 2 = Female, 9 = Other.
Line Feed	1	237	0x0A
Height Header	3	238-240	“DAU”
Height Field	3	241-243	Height in format FeetInches e.g. 511
Line Feed	1	244	0x0A
Eye Color Header	3	245-247	“DAY”
Eye Color Field	3	248-250	Eye color
Line Feed	1	251	0x0A
Social Number Header	3	252-254	“DBK”
Social Number Field	9	255-263	BLANK
Line Feed	1	264	0x0A
Organ Donor Header	3	265-267	“DBH”
Organ Donor Field	9	268-276	Organ Donor

Licenses Issued between October 21st 2005 and January 11th 2006

Length 278 Bytes.

Changes to the previous version:

- Increased Barcode length to 278 Characters
- Donor field increased back to 10 characters
- Carriage Return character placed at end of barcode

Field	Length	Byte Position	Value
Start Character	1	1	'@'
Line Feed	1	2	0x0A
Record Separator	1	3	0x1C
Carriage Return	1	4	0x0D
File Type	5	5-9	"AAMVA"
Jurisdiction Code	5	10-14	"36001"
Version Number	1	15	"0"
Sub Files	2	16-17	"01"
Sub File Header	10	18-27	"DL00270249"
Sub File ID	2	28-29	"DL"
Line Feed	1	30	0x0A
Name Header	3	31-33	"DAA"
Name Field	35	34-68	Name Field with commas translated to '@'
Line Feed	1	69	0x0A
Street Header	3	70-72	"DAG"
Street Field	20	73-92	Address Street Information
Line Feed	1	93	0x0A
City Header	3	94-96	"DAI"
City Field	15	97-111	Address City Information
Line Feed	1	112	0x0A
State Header	3	113-115	"DAJ"
State Field	2	116-118	"NY"
Line Feed	1	119	0x0A
Zip Code Header	3	120-122	"DAK"
Zip Code Field	11	123-132	Address Zip Code Information
Line Feed	1	133	0x0A
License Number Header	3	134-136	"DAQ"
License Number Field	25	137-161	License Number
Line Feed	1	162	0x0A
Date of Birth Header	3	163-165	"DBB"
Date of Birth Field	8	166-173	Date of birth in the format yyyymmdd

Electronic Ticket/Accident Reporting Specifications

Field	Length	Byte Position	Value
Line Feed	1	174	0x0A
Date of Issue Header	3	175-177	“DBD”
Date of Issue Field	8	178-185	Date of issue in the format yyyymmdd
Line Feed	1	186	0x0A
Date of Expiry Header	3	187-189	“DBA”
Date of Expiry Field	8	190-197	Date of Expiry in the format yyyymmdd
Line Feed	1	198	0x0A
Document Class Header	3	199-201	“DAR”
Document Class Field	4	202-205	Document Class
Line Feed	1	206	0x0A
Restriction Header	3	207-209	“DAS”
Restriction Field	10	210-219	Restrictions
Line Feed	1	220	0x0A
Endorsement Header	3	221-223	“DAT”
Endorsement Field	8	224-231	Endorsements
Line Feed	1	232	0x0A
Gender Header	3	233-335	“DBC”
Gender Field	1	236	Gender Code. 0 = Unknown, 1 = Male, 2 = Female, 9 = Other.
Line Feed	1	237	0x0A
Height Header	3	238-240	“DAU”
Height Field	3	241-243	Height in format FeetInches e.g. 511
Line Feed	1	244	0x0A
Eye Color Header	3	245-247	“DAY”
Eye Color Field	3	248-250	Eye color
Line Feed	1	251	0x0A
Social Number Header	3	252-254	“DBK”
Social Number Field	9	255-263	BLANK
Line Feed	1	264	0x0A
Organ Donor Header	3	265-267	“DBH”
Organ Donor Field	10	268-277	Organ Donor
Carriage Return	1	278	0x0D

Licenses Issued after January 11th 2006

Length 278 Bytes.

Changes to the previous version:

- Increased Barcode length in the 'DL' Sub File header to 251 Characters

Field	Length	Byte Position	Value
Start Character	1	1	'@'
Line Feed	1	2	0x0A
Record Separator	1	3	0x1C
Carriage Return	1	4	0x0D
File Type	5	5-9	"AAMVA"
Jurisdiction Code	5	10-14	"36001"
Version Number	1	15	"0"
Sub Files	2	16-17	"01"
Sub File Header	10	18-27	"DL00270251"
Sub File ID	2	28-29	"DL"
Line Feed	1	30	0x0A
Name Header	3	31-33	"DAA"
Name Field	35	34-68	Name Field with commas translated to '@'
Line Feed	1	69	0x0A
Street Header	3	70-72	"DAG"
Street Field	20	73-92	Address Street Information
Line Feed	1	93	0x0A
City Header	3	94-96	"DAI"
City Field	15	97-111	Address City Information
Line Feed	1	112	0x0A
State Header	3	113-115	"DAJ"
State Field	2	116-118	"NY"
Line Feed	1	119	0x0A
Zip Code Header	3	120-122	"DAK"
Zip Code Field	11	123-132	Address Zip Code Information
Line Feed	1	133	0x0A
License Number Header	3	134-136	"DAQ"
License Number Field	25	137-161	License Number
Line Feed	1	162	0x0A
Date of Birth Header	3	163-165	"DBB"
Date of Birth Field	8	166-173	Date of birth in the format yyyymmdd
Line Feed	1	174	0x0A
Date of Issue Header	3	175-177	"DBD"
Date of Issue Field	8	178-185	Date of issue in the format

Electronic Ticket/Accident Reporting Specifications

Field	Length	Byte Position	Value
			yyyymmdd
Line Feed	1	186	0x0A
Date of Expiry Header	3	187-189	“DBA”
Date of Expiry Field	8	190-197	Date of Expiry in the format yyyymmdd
Line Feed	1	198	0x0A
Document Class Header	3	199-201	“DAR”
Document Class Field	4	202-205	Document Class
Line Feed	1	206	0x0A
Restriction Header	3	207-209	“DAS”
Restriction Field	10	210-219	Restrictions
Line Feed	1	220	0x0A
Endorsement Header	3	221-223	“DAT”
Endorsement Field	8	224-231	Endorsements
Line Feed	1	232	0x0A
Gender Header	3	233-335	“DBC”
Gender Field	1	236	Gender Code. 0 = Unknown, 1 = Male, 2 = Female, 9 = Other.
Line Feed	1	237	0x0A
Height Header	3	238-240	“DAU”
Height Field	3	241-243	Height in format FeetInches e.g. 511
Line Feed	1	244	0x0A
Eye Color Header	3	245-247	“DAY”
Eye Color Field	3	248-250	Eye color
Line Feed	1	251	0x0A
Social Number Header	3	252-254	“DBK”
Social Number Field	9	255-263	BLANK
Line Feed	1	264	0x0A
Organ Donor Header	3	265-267	“DBH”
Organ Donor Field	10	268-277	Organ Donor
Carriage Return	1	278	0x0D

New York State Registration Barcode Format

Vehicle Registration

There will be two (2) bar codes on the Vehicle Registration documents. These symbologies will be the linear code (USS-128B) presently used on the registration document, and a new code (PDF-417).

Present Linear Registration Barcode

Start Code

Data Identifier - (4)

Vehicle Year - 2 Numeric

Vehicle Make - 2 Numeric (Vehicle make code – **see table at end of this chapter**)

Cylinders - 1 Numeric (Cylinders - 0 = Rotary, 1-8, 9 = 9 or more cyl.)

Weight Code - 1 Numeric Weight code - 1 = 0-8500, 2 = 8501-10000, 3 = 10001-18000,
4 = 18001 and more

Fuel Code - 1 Numeric (1 = Gas, 2 = Non Gas, 3 = None)

NYMA Code - 1 Numeric (1 = NYMA, 2 = Outside NYMA)

Registration Class- 2 Numeric

Plate Number - (maximum eight alpha/numeric)

The number of characters filled will depend on the number of characters in the license plate. Only those characters on the vehicle license plate will be bar coded (no spaces).

Check Character

Stop Code

Two Dimensional Bar Codes (PDF417)

Registration Sticker -

The PDF417 Barcode on the New York Registration document will be produced in conformance with the March 1996, AAMVA Compliant PDF417 document. DMV has issued two versions of the registration barcode. The test system should be capable of reading and decoding both.

Version 1 follows: (August 1996)

**AMVA Bar-code Example
(08/13/96)**

Bytes	Literal	Variable	Description
(Header)			
1- 1	@		Compliance Indicator
2- 2	l/f		Data Element Separator
3- 3	r/s		Record Separator
4- 4	c/r		Segment Terminator
5- 9	AAMVA		File Type
10- 14		36001	Jurisdiction Code
15- 15	0		Version Number
16- 17		04	Number of Subfiles
(Subfile Designator - One per Subfile)			
18- 19	VH		Subfile Type (vehicle)
20- 23		0057	Offset
24- 27		0063	Length of subfile
28- 29	RG		Subfile Type (reg.)
30- 33		0120	Offset
34- 37		0023	Length of subfile
38- 39	ZV		Subfile Type (NY-Dev veh)
40- 43		0143	Offset
44- 47		0028	Length of subfile
48- 49	ZR		Subfile Type (NY-Def reg)
50- 53		0171	Offset
54- 57		0015	Length of subfile
(Subfile - Vehicle Record)			
58- 59	VH		Start Vehicle subfile
60- 63	l/fVAD		Vin Number follows
64- 80		1G1JC81W7J1111111	
81- 84	l/fVAK		Make follows
85- 88		CHEV	(NCIC seems to be req'd)
89- 92	l/fVAL		Year follows

Electronic Ticket/Accident Reporting Specifications

93- 94		88	
95- 98	l/fVAN		Fuel follows
99- 99		G	
100-103	l/fVAQ		No. of Cylinders follows
104-106		006	
107-110	l/fVAT		Weight follows
111-119		002607 LB	
120-120	c/r		End Vehicle subfile

(Subfile - Registration)

121-122	RG		Begin Reg. subfile
123-126	l/fRAL		Plate Class follows
127-130		PAS	
131-134	l/fRAM		Plate Number follows
135-142		ABC1234	
143-143	c/r		End reg. subfile

(Subfile - NYDMV-Defined Vehicle-related fields)

144-145	ZV		Begin NY-Defined Veh.
146-149	l/fZVA		NY-Defined year follows
150-153		1988	(full four digit year) 154-
157	l/fZVB		NY-Defined Make follows
158-162		CHEVR	(Chevrolet)
163-166	l/fZVC		NY-Defined Body follows
167-170		SUBN	(station wagon)
171-171	c/r		End of file

(Subfile - NYDMV-Defined Registration-related fields)

172-173	ZR		Begin NY-Defined Reg.
174-177	l/fZRA		NYMA Indicator follows
178-178		2	(vehicle is not in NYMA)
179-182	l/fZRB		Three-Of-Name follows
183-185		MOT	
186-186	c/r		End NY-Defined Reg.

Observations on the above:

- 1) NYMA had to be defined as its own subfile, because there was no corresponding identifier in the rest of the specs. The "ZA" through "ZZ" subfile types are left by AAMVA for jurisdictions to define. The DMV-encoded body type appears here, as well.
- 2) The above layout is very subject to change.
- 3) The make code will be translated using a table of DMV-encoded makes and NCIC makes. Where a match is not found, we will place "XXXX" (unable to translate) into the field. The five-

character make, as it appears on our file, will be encoded in the "DMV Defined" area of the bar-code.

Version 2 follows:

**AMVA Bar-code Example
(05/14/97)**

Bytes	Literal	Variable	Description
(Header)			
1- 1	@		Compliance Indicator
2- 2	l/f		Data Element Separator
3- 3	r/s		Record Separator
4- 4	c/r		Segment Terminator
5- 9	AAMVA		File Type
10- 14		36001	Jurisdiction Code
15- 15	0		Version Number
16- 17		05	Number of Subfiles
(Subfile Designator - One per Subfile)			
18- 19	VH		Subfile Type (vehicle)
20- 23		0067	Offset
24- 27		0058	Length of subfile
28- 29	RG		Subfile Type (reg.)
30- 33		0125	Offset
34- 37		0037	Length of subfile
38- 39	ZV		Subfile Type (NY-Dev veh)
40- 43		0162	Offset
44- 47		0042	Length of subfile
48- 49	ZR		Subfile Type (NY-Def reg)
50- 53		0204	Offset
54- 57		0015	Length of subfile
58- 59	ZZ		Subfile Type (NY-Def ver)
60- 63		0219	Offset
64- 67		0013	Length of subfile
(Subfile - Vehicle Record)			
68- 69	VH		Start Vehicle subfile
70- 73	l/fVAD		Vin Number follows
74- 90		1G1JC81W7J1111111	
91- 94	l/fVAK		Make follows
95- 98		CHEV	(NCIC seems to be req'd)
99-102	l/fVAL		Year follows
103-104		88	

Electronic Ticket/Accident Reporting Specifications

105-108	1/fVAQ		No. of Cylinders follows
109-111		006	
112-115	1/fVAT		Weight follows
116-124		002607 LB	
125-125	c/r		End Vehicle subfile

(Subfile - Registration)

126-127	RG		Begin Reg. subfile
128-131	1/fRAG		Reg. Exp. Date follows
132-141		19990430	
142-145	1/fRAL		Plate Class follows
146-149		PAS	
150-153	1/fRAM		Plate Number follows
154-161		ABC1234	
162-162	c/r		End reg. subfile

(Subfile - NYDMV-Defined Vehicle-related fields)

163-164	ZV		Begin NY-Defined Veh.
165-168	1/fZVA		NY-Defined year follows
169-172		1988	(full four digit year)
173-176	1/fZVB		NY-Defined Make follows
177-181		CHEVR	(Chevrolet)
182-185	1/fZVC		NY-Defined Body follows
186-189		SUBN	(station wagon)
190-193	1/fZVD		NY-Defined Fuel follows
194-194		G	Allowable Fuels are:
			G - Gasoline
			D - Diesel
			E - Electric
			P - Propane
			C - Comp. Nat. Gas
			F - Flex
195-198	1/fZVE		NY-Defined Color Follows
199-203		DK/RD	(as defined in VIDIO
			Training Manual)
204-204	c/r		End of file

(Subfile - NYDMV-Defined Registration-related fields)

205-206	ZR		Begin NY-Defined Reg.
207-210	1/fZRA		NYMA Indicator follows
211-211		2	(vehicle is not in NYMA)
212-215	1/fZRB		Three-Of-Name follows
216-218		MOT	
219-219	c/r		End NY-Defined Reg.

Electronic Ticket/Accident Reporting Specifications

(Subfile - NYDMV-Defined Version Control Info.)

220-221	ZZ		Begin NY-Defined V. Ctl.
222-225	1/fZZZ		Barcode Version follows
226-231		199706	(Year and month of rev.) 232-
232	c/r		End NY-Defined V. Ctl.

Changes From August, 1996 Version

- 1) Fuel moved from main Vehicle portion to NY-Defined Vehicle portion, to accommodate new non-AAMVA-standard fuel codes.
- 2) Reg. Expiration Date field added
- 3) NY-Defined Vehicle Color added
- 4) Version of barcode (199606) appears at end of barcode, in "ZZZ" field.

File length changed from 186 to 232 characters as a result of the above changes.

Tables needed to decode linear barcode vehicle information

Linear Barcode USS-128B tables for Vehicle Make, Vehicle Weight Code, NYMA code and Fuel type code are:

Vehicle Make - Two digit codes for each vehicle make listed below will be part of the USS-128B bar code on the vehicle registration. Record storage will be the first 5 letters of the vehicle make as noted in the table below.

01-ACURA	11-DATSU	21-JAGUA	31-MITSU	41-ROVER	51-LEXUS
02-AL/RO	12-DODGE	22-JEEP	32-NISSA	42-SAAB	52-EAGLE
03-AMERI	13-FERRA	23-LANCI	33-OLDSM	43-STERL	53-GEO
04-AUDI	14-FIAT	24-LINCO	34-OPEL	44-SUBAR	54-INFIN
05-BMW	15-FORD	25-LOTUS	35-PEUGE	45-SUZUK	55-SATUR
06-BUICK	16-GMC	26-MASER	36-PLYMO	46-TOYOT	56-DIHAT
07-CADIL	17-HONDA	27-MAZDA	37-PONTI	47-TRIUM	57-OTHER
08-CHECK	18-HYUND	28-ME/BE	38-PORSC	48-VOLKS	
09-CHEVR	19-INTER	29-MERCU	39-RENAU	49-VOLVO	
10-CHRY	20-ISUZU	30-MG	40-RO/RO	50-YUGO	

Vehicle Weight Code - The computer shall store a table to convert a weight entered through the keyboard or linear barcode into a single digit code, or to convert the vehicle weight returned from the DMV registration file into the appropriate code.

Code 1= Vehicles with a weight of less than 8501.

Code 2= Vehicles with a weight greater than 8500 through 10000 lbs.

Code 3= Vehicles with a weight greater than 10000 and less than 18,001.

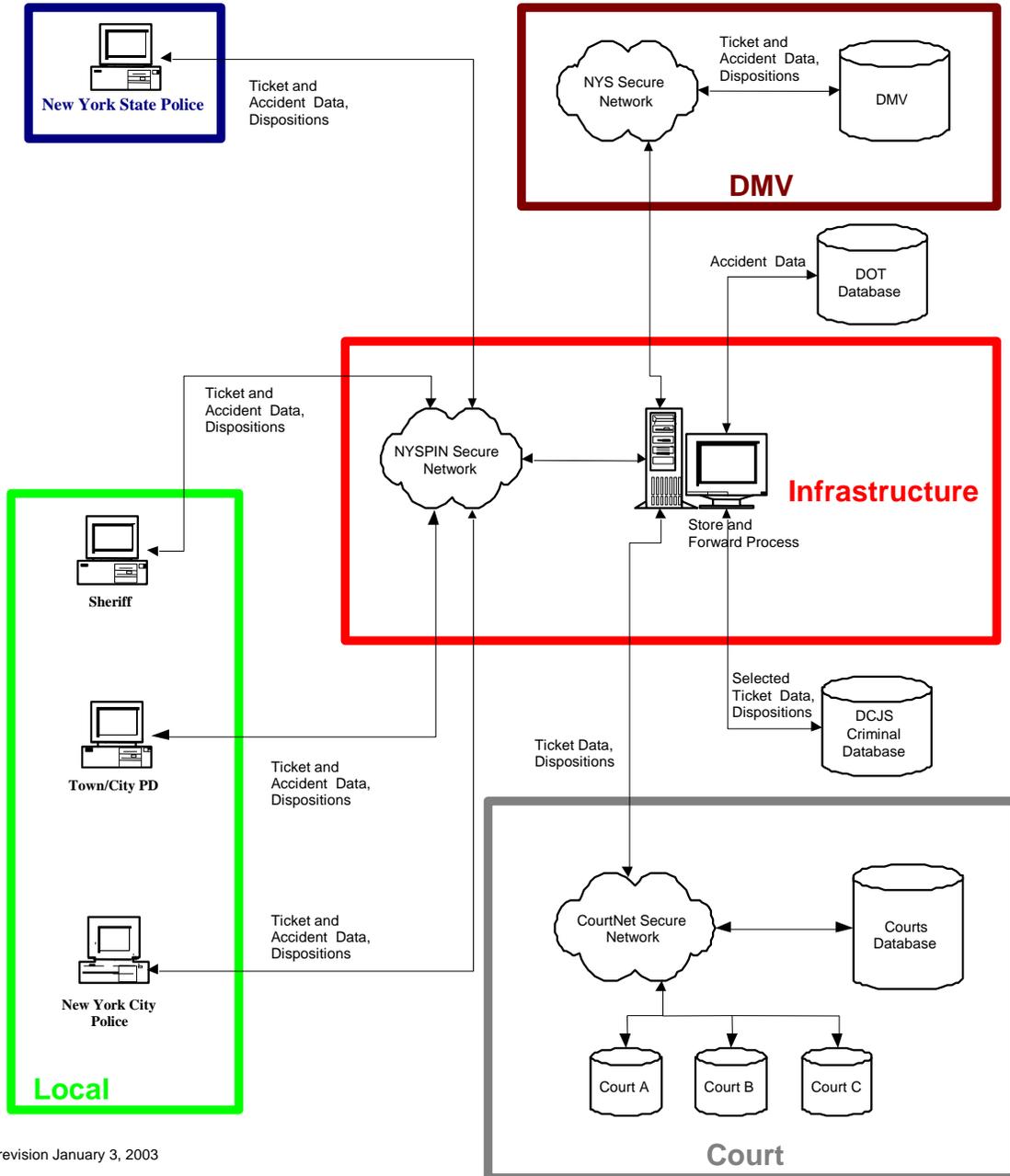
Code 4= Vehicles with a weight greater than 18,000 and buses with a seating capacity greater than 15.

Fuel Type Code - The computer will have a table to convert the type of fuel used in a vehicle.

1=Gasoline 2=Non-Gasoline 3=None (trailer)

Attachment A- Context Diagram

New York State Electronic Ticketing / Accident Report Context Diagram



revision January 3, 2003

Attachment B- Agency and Vendor Contact Information

New York State Department of Motor Vehicles

Application for Participation in the NY State Police/NYS DMV Electronic Ticket/Accident Reporting Program

APPLICANT ORGANIZATION

Law Enforcement Agency Name and Contact Information

Enter the official name and mailing address of the applicant organization:

Agency Name: _____
Street Address: _____

City: _____
State: _____
Zip Code: _____
Telephone & Ext: _____
Fax: _____
E-Mail Address: _____

Primary Contact Person

Enter a name and contact information for the person who will be the primary point of contact with DMV:

Contact Name: _____
Title: _____
Telephone & Ext: _____
Fax: _____
E-Mail Address: _____

VENDOR INFORMATION

Complete this section to indicate if you are currently using, or are planning to use, a vendor's services or software to submit electronic ticket and/or accident reporting transactions to DMV.

Select the option that best describes your organization's plans for using a vendor:

- We do not plan to use a vendor (developing software in-house.)
- We are planning to use a vendor but have not selected one yet.
- We are planning to use the vendor identified below.

Vendor Name and Address

Enter the vendor's name and contact information here:

Vendor's Business
Name: _____

Vendor Contact Name: _____

Title: _____

Street Address: _____

City: _____

State: _____

Zip Code: _____

Telephone: _____

Fax: _____

E-Mail Address: _____

Do you currently use this vendor to help you submit transactions to DMV?

Yes No

Vendor Services

What kind of services does/will the vendor provide? (check all that apply):

- The vendor submits transactions to DMV on behalf of the organization.
- The vendor provides software or systems that enable the organization to submit its own transactions directly to DMV.
- Other (please explain below):

Return the completed application form to:

NYS Dept. of Motor Vehicles
Program Analysis
6 ESP, Room 530
Albany, New York 12228
Attention: Electronic Ticket/Accident Reporting Coordinator

Attachment C- TraCS Local Lead Agencies

For each county, there is a local lead agency for TraCS that new agencies can coordinate with, and who can answer any questions regarding the TraCS forms.

AGENCY	ADDRESS	TELEPHONE	CONTACT
Albany			
Albany City Police Dept	165 Henry Johnson Blvd Albany, NY 12210-1525	(518) 462-8000	Sgt William Dobbs (518) 447-8794 wdobbs@albany-ny.org
Allegany			
Allegany Co Sheriff's Dept	7 Court Street Belmont, NY 14813	(585) 268-9204	Keith Hooker (585) 268-9802 hookerkm@alleganyco.com
Broome			
Broome Co Sheriff's Office	155 Lt VanWinkle Drive Binghamton, NY 13905	(607) 778-1911	Sgt Mark Oliver (607) 778-8726 moliver@co.broome.ny.us
Cayuga			
Auburn City Police Dept	46 North St Auburn, NY 13021	(315) 255-2621	PO / IT Admin Josh Middleton (315) 255-2621 rckid@adelphia.net
Chautauqua			
Chautauqua Co Sheriffs Dept	PO Box 128 Mayville, NY 14757	(716) 753-2131	Tech Sgt Vincent Gerace (716) 753-2131 vg@sheriff.us
Dutchess			
Dutchess Co Sheriff's Office	150 North Hamilton Street Poughkeepsie, NY 12601	(914) 486-3800	Sgt Robert Monaco (845) 486-3871 ramonaco@co.dutchess.ny.us
Erie			
Erie County Central Police Service	45 Elm Street, Room 222 Buffalo, NY 14203	(716) 858-7461	TraCS Coordinator Susanne Spencer (716) 858-2767 spencers@erie.gov
Genesee			
Genesee Co Sheriff's Dept	14 West Main Batavia, NY 14021-0151	(585) 343-0911	Chief Deputy Gordon Dibble (585) 345-3000 gdibble@co.genesee.ny.us
Livingston			
Livingston Co Sheriffs Dept	4 Court St Geneseo, NY 14454	(585) 243-7100	IS Coordinator Quinton Taylor (585) 243-7114 qtaylor@co.livingston.ny.us IS Director Dale Nieswiadomy (585) 243-7113 dnieswiadomy@co.livingston.ny.us
Madison			
Madison Co Sheriff's Dept	Po Box 16 North Court St Wampsville, NY 13163	(315) 366-2318	Lt. Mark McLean (315) 366-2466 mark.mclean@co.madison.ny.us
Monroe			
Monroe County Sheriff's Office	130 Plymouth Avenue South Rochester, NY 14614	(585) 428-5245	Holly Gudonis (585) 753-4711 hgudonis@monroecounty.gov
Rochester City Police Dept	185 Exchange Blvd Rochester, NY 14614	(585) 428-6402	Lt/CIO Mike Kozak (585) 428-7335 mk0130@cityofrochester.gov DBA James Hawkins (585) 428-7333 jh1286@cityofrochester.gov

Electronic Ticket/Accident Reporting Specifications

AGENCY	ADDRESS	TELEPHONE	CONTACT
Nassau			
Nassau Co. Police Dept.	1490 Franklin Ave Mineola, NY 11501	(516) 573-7600	Officer Michael LoRe (516) 573-7481 (516) 573-7481
Nassau County Traffic Safety Board	1550 Franklin Avenue Room 111 Mineola NY 11501		(516) 571-5033 Christopher.Mistron@mail.co.na
Oneida			
Utica City Police Dept.	413 Oriskany St. West Utica, NY 13502	(315) 735-3301	Sgt Tony Martino (315) 223-3590 amartino@uticapd.com
Onondaga			
Onondaga County 911 Center			DBA Ken DeFilipps (315) 335-1602 ken@mapolce.com
Ontario			
Ontario Co Sheriff's Office	74 Onatrio Street Canandaigua, NY 14424	(585) 394-4560	Sr Programmer Kevin Erdle (585) 396-4506 kevin.erdle@co.ontario.ny.us
Orange			
Monroe Village Police Dept	104 Stage Road Monroe, NY 10950	(845) 782-8644	Officer Gregory Witte (845) 782-8644 gwwitte@monroepd.org
Orleans			
Orleans Co Sheriff's Dept.	13925 SR 31, Suite 400 Albion, NY 14411	(585) 589-5527	Deputy Sheriff Theo Gunkler (585) 506-7240 gunklert@orleansny.com
Otsego			
Otsego Co Sheriff's Dept	RD 4 Box 398A 172 Co Hwy 33 W Cooperstown, NY 13326	(607) 547-4271	Sgt Richard Devlin (607) 547-4273 devlinr@otsegocounty.com
Rensselaer			
Troy City Police Dept	55 State Street Troy, NY 12180	(518) 270-4411	Tech Advisor Tenn Chen (518) 270-4544 Tenn.Chen@troyny.gov Captain Paul Bouchard (518) 270-4427 paul.bouchard@troyny.gov
Rockland			
Clarkstown Town Police Dept	20 Maple Ave New City, NY 10956	(845) 639-5800	Communications Coordinator Karl Muller (845) 639-5872 k_muller@town.clarkstown.ny.us
Saratoga			
Mechanicville City Police Dept	36 No. Main St Mechanicville, NY 12118	(518) 664-7383	Lt David Gonnely (518) 664-7383 ltmpd@nycap.rr.com
Schenectady			
Rotterdam Town Police Dept	101 Princetown Rd Schenectady, NY 12306	(518) 355-7331	Patrolman Robert Dufek (518) 355-7331 rdufek@nycap.rr.com
Schoharie			
Cobleskill Village Police Dept	378 Mineral Springs Rd Cobleskill, NY 12043	(518) 234-2923	Sgt Lawrence Travis (518) 234-2923 lmt201@midtel.net Patrolman Jeffery Brown (518) 234-2923 tracs@jafadog.com
Schuyler			
Schuyler County Sheriff's Dept	106 10th Street Watkins Glen, NY 14891	(607) 535-8222	Sgt Todd Day (607) 535-8222

Electronic Ticket/Accident Reporting Specifications

AGENCY	ADDRESS	TELEPHONE	CONTACT
St. Lawrence Massena Village Police Dept	60 Main Street Suite 1 Massena, NY 13662	(315) 769-3577	Investigator Joe Brown(315) 764-5508 jbrown@police.massena.ny.us
State Agency NYC Department of Environmental	59-17 Junction Blvd., 19th Flr Flushing, NY 11373	(315) 769-3577	Investigator Joe Brown (315) 764-5508 rick.marsan@hp.com
Steuben Steuben County Sheriff's Dept	7007 Rumsey St. Ext. Bath, NY 14810	(607) 776-7009	Chief Deputy Joel Ordway (800) 724-7777 ordwayjr@co.steuben.ny.us
Suffolk Riverhead Town Police Dept	210 Howell Avenue Riverhead, NY 11901	631-727-4500	Captain Richard Smith (631) 727-4500 rts@riverheadli.com
Ulster Ulster Co. Sheriff's Dept	129 Schwenk Drive Kingston, NY 12401	(845) 338-3640	Asst Dir Chris Fiore (845) 340-5390 cfio@co.ulster.ny.us
Warren Glens Falls City Police Dept	42 Ridge St Glens Falls, NY 12801	(518) 761-3840	Sgt Rob Ash (518) 761-0000 rash@glensfallspd.com
Wayne Wayne Co Sheriff's Dept	7368 Route 31 Lyons, NY 14489	(315) 946-5776	Lt. Bob Hetzke (315) 946-5776 bhetzke@co.wayne.ny.us
Westchester Westchester Co Dept Public Safety	1 Saw Mill River Parkway Hawthorne, NY 10532	(914) 741-4400	Sergeant James Welsh (914) 864-7848 jaw1@westchestergov.com Kelly Odestick (914) 995-5155 kac2@westchestergov.com
Wyoming Perry Village Police Dept	P.O. Box 253 Perry, NY 14530		Officer Anthony Ciravola apciravola@villageofperry.com
Yates Yates County Sheriff's Dept	227 Main Street Penn Yan, NY 14527	(315) 536-4438	Sgt Patrick Killen pkillen@yatescounty.org

Standardized Reports

Investigation Report
Supplemental Report
Arrest Report
Warrant Activity Report
UCR/IBR Crime Reports by County and for all Counties, including Arson, Hate Crime, and Homicide.
Chain of Custody Report (Individual Item and for a Case)
Fingerprint Card

Supervisory Reports:

Cases submitted to you awaiting Review
Cases returned for correction
Open Cases by TZS
Open Cases by Member
Open Cases by Supervisor
Case with PPD (Open and Closed)
PPD Court – going forward should be part of above report
Property/Evidence Inventory by location
Warrants – Active, by assigned Member, TZS
Closed and not locked – should be accounted for in workflow- right?
BCI – Case adoptions
BCI Cases not yet adopted (7 days TOT – BCI)
Applicant – Status Report
NYPTI Late Report – Closed by arrest but not sent to DA.
PIO Report – Daily

Activity Reports (Uniform and BCI):

Daily, Weekly, Monthly Activity Reports from Member through Division (must account for “accurate number reporting” per day average, per station average Troop Average.)

INFORMATION SHARING ENVIRONMENT (ISE)
FUNCTIONAL STANDARD (FS)
SUSPICIOUS ACTIVITY REPORTING (SAR)
VERSION 1.5

1. Authority. Homeland Security Act of 2002, as amended; The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended; Presidential Memorandum dated April 10, 2007 (Assignment of Functions Relating to the Information Sharing Environment); Presidential Memorandum dated December 16, 2005 (Guidelines and Requirements in Support of the Information Sharing Environment); DNI memorandum dated May 2, 2007 (Program Manager's Responsibilities); Executive Order 13388; and other applicable provisions of law, regulation, or policy.
2. Purpose. This issuance serves as the updated Functional Standard for ISE-SARs, and one of a series of Common Terrorism Information Sharing Standards (CTISS) issued by the PM-ISE. While limited to describing the ISE-SAR process and associated information exchanges, information from this process may support other ISE processes to include alerts, warnings, and notifications, situational awareness reporting, and terrorist watchlisting.
3. Applicability. This ISE-FS applies to all departments or agencies that possess or use terrorism or homeland security information, operate systems that support or interface with the ISE, or otherwise participate (or expect to participate) in the ISE, as specified in Section 1016(i) of the IRTPA.
4. References. ISE Implementation Plan, November 2006; ISE Enterprise Architecture Framework (EAF), Version 2.0, September 2008; Initial Privacy and Civil Liberties Analysis for the Information Sharing Environment, Version 1.0, September 2008; ISE-AM-300: Common Terrorism Information Standards Program, October 31, 2007; Common Terrorism Information Sharing Standards Program Manual, Version 1.0, October 2007; National Information Exchange Model, Concept of Operations, Version 0.5, January 9, 2007; 28 Code of Federal Regulations (CFR) Part 23; Executive Order 13292 (Further Amendment to Executive Order 12958, as Amended, Classified National Security Information); Nationwide Suspicious Activity Reporting Concept of Operations, December 2008; ISE Suspicious Activity Reporting Evaluation Environment (EE) Segment Architecture, December 2008.
5. Definitions.
 - a. Artifact: Detailed mission product documentation addressing information exchanges and data elements for ISE-SAR (data models, schemas, structures, etc.).

- b. CTISS: Business process-driven, performance-based “common standards” for preparing terrorism information for maximum distribution and access, to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE. CTISS, such as this *ISE-SAR Functional Standard*, are implemented in ISE participant infrastructures that include ISE Shared Spaces as described in the *ISE EAF*. Two categories of common standards are formally identified under CTISS:
 - (1) Functional Standards – set forth rules, conditions, guidelines, and characteristics of data and mission products supporting ISE business process areas.
 - (2) Technical Standards – document specific technical methodologies and practices to design and implement information sharing capability into ISE systems.
- c. Information Exchange: The transfer of information from one organization to another organization, in accordance with CTISS defined processes.
- d. ISE-Suspicious Activity Report (ISE-SAR): An ISE-SAR is a SAR (as defined below in 5i) that has been determined, pursuant to a two-part process, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism). ISE-SAR business, privacy, and civil liberties rules will serve as a unified process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.
- e. National Information Exchange Model (NIEM): A joint technical and functional standards program initiated by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) that supports national-level interoperable information sharing.
- f. Personal Information: Information that may be used to identify an individual (i.e., data elements in the identified “privacy fields” of this *ISE-SAR Functional Standard*).
- g. Privacy Field: A data element that may be used to identify an individual and, therefore, may be subject to privacy protection.
- h. Suspicious Activity: Observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
- i. Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.
- j. Universal Core (UCore): An interagency information exchange specification and implementation profile. It provides a framework for sharing the most commonly used data concepts of “who, what when, and where”. UCore serves as a starting point for data level integration and permits the development of richer domain specific exchanges. UCore was developed in concert with NIEM program office, and is a collaborative effort between Department of Defense (DOD), DOJ, DHS and the Intelligence Community.

6. Guidance. This Functional Standard is hereby established as the nationwide ISE Functional Standard for ISE-SARs. It is based on documented information exchanges and business requirements, and describes the structure, content, and products associated with processing, integrating, and retrieving ISE-SARs by ISE participants.

7. Responsibilities.

- a. The PM-ISE, in consultation with the Information Sharing Council (ISC), will:
 - (1) Maintain and administer this *ISE-SAR Functional Standard*, to include:
 - (a) Updating the business process and information flows for ISE-SAR.
 - (b) Updating data elements and product definitions for ISE-SAR.
 - (2) Publish and maintain configuration management of this *ISE-SAR Functional Standard*.
 - (3) Assist with the development of ISE-SAR implementation guidance and governance structure, as appropriate, to address privacy, civil rights, and civil liberties, policy, architecture, and legal issues.
 - (4) Work with ISE participants, through the CTISS Committee, to develop a new or modified *ISE-SAR Functional Standard*, as needed.
 - (5) Coordinate, publish, and monitor implementation and use of this *ISE-SAR Functional Standard*, and coordinate with the White House Office of Science and Technology Policy and with the National Institute of Standards and Technology (in the Department of Commerce) for broader publication, as appropriate.
- b. Each ISC member and other affected organizations shall:
 - (1) Propose modifications to the PM-ISE for this Functional Standard, as appropriate.
 - (2) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with relevant current (operational) mission specific programs, systems, or initiatives (e.g. operations and maintenance {O&M} or enhancements).
 - (3) As appropriate, incorporate this *ISE-SAR Functional Standard*, and any subsequent implementation guidance, into budget activities associated with future or new development efforts for relevant mission specific programs, systems, or initiatives (e.g. development, modernization, or enhancement {DME}).
 - (4) Ensure incorporation of this *ISE-SAR Functional Standard*, as set forth in 7.b (2) or 7.b (3) above, is done in compliance with ISE Privacy Guidelines and any additional guidance provided by the ISE Privacy Guidelines Committee.

8. Effective Date and Expiration. This ISE-FS is effective immediately and will remain in effect as the updated *ISE-SAR Functional Standard* until further updated, superseded, or cancelled.

A handwritten signature in black ink, appearing to read "Thomas E. McManis". The signature is written in a cursive style with a horizontal line underneath it.

Program Manager for the
Information Sharing Environment

Date: May 21, 2009

PART A – ISE-SAR FUNCTIONAL STANDARD ELEMENTS

SECTION I – DOCUMENT OVERVIEW

A. List of ISE-SAR Functional Standard Technical Artifacts

The full ISE-SAR information exchange contains five types of supporting technical artifacts. This documentation provides details of implementation processes and other relevant reference materials. A synopsis of the *ISE-SAR Functional Standard* technical artifacts is contained in Table 1 below.

Table 1 – Functional Standard Technical Artifacts¹

Artifact Type	Artifact	Artifact Description
Development and Implementation Tools	1. Component Mapping Template (CMT) (SAR-to-NIEM/UCore)	This spreadsheet captures the ISE-SAR information exchange class and data element (source) definitions and relates each data element to corresponding National Information Exchange Model (NIEM) Extensible Mark-Up Language (XML) elements and UCore elements, as appropriate.
	2. NIEM Wantlist	The Wantlist is an XML file that lists the elements selected from the NIEM data model for inclusion in the Schema Subset. The Schema Subset is a compliant version to both programs that has been reduced to only those elements actually used in the ISE-SAR document schema.
	3. XML Schemas	The XML Schema provides a technical representation of the business data requirements. They are a machine readable definition of the structure of an ISE-SAR-based XML Message.
	4. XML Sample Instance	The XML Sample Instance is a sample document that has been formatted to comply with the structures defined in the XML Schema. It provides the developer with an example of how the ISE-SAR schema is intended to be used.
	5. Codified Data Field Values	Listings, descriptions, and sources as prescribed by data fields in the <i>ISE-SAR Functional Standard</i> .

¹ Development and implementation tools may be accessible through www.ise.gov. Additionally, updated versions of this Functional Standard will incorporate the CTISS Universal Core which harmonizes the NIEM Universal Core with the DoD/IC UCore.

SECTION II – SUSPICIOUS ACTIVITY REPORTING EXCHANGES

A. ISE-SAR Purpose

This *ISE-SAR Functional Standard* is designed to support the sharing, throughout the Information Sharing Environment (ISE), of information about suspicious activity, incidents, or behavior (hereafter collectively referred to as suspicious activity or activities) that have a potential terrorism nexus. The ISE includes State and major urban area fusion centers and their law enforcement,² homeland security,³ or other information sharing partners at the Federal, State, local, and tribal levels to the full extent permitted by law. In addition to providing specific indications about possible terrorism-related crimes, ISE-SARs can be used to look for patterns and trends by analyzing information at a broader level than would typically be recognized within a single jurisdiction, State, or territory. Standardized and consistent sharing of suspicious activity information regarding criminal activity among State and major urban area fusion centers and Federal agencies is vital to assessing, deterring, preventing, or prosecuting those involved in criminal activities associated with terrorism. This *ISE-SAR Functional Standard* has been designed to incorporate key elements that describe potential criminal activity associated with terrorism and may be used by other communities to address other types of criminal activities where appropriate.

B. ISE-SAR Scope

Suspicious activity is defined as *observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity*. A determination that such suspicious activity constitutes an ISE-SAR is made as part of a two-part process by trained analysts using explicit criteria. Some examples of the criteria for identifying those SARs, with defined relationships to criminal activity that also have a potential terrorism nexus, are listed below. Part B (ISE-SAR Criteria Guidance) provides a more thorough explanation of ISE-SAR criteria, highlighting the importance of context in interpreting such behaviors;

- Expressed or implied threat
- Theft/loss/diversion
- Site breach or physical intrusion
- Cyber attacks
- Probing of security response

² All references to Federal, State, local and tribal law enforcement are intended to encompass civilian law enforcement, military police, and other security professionals.

³ All references to homeland security are intended to encompass public safety, emergency management, and other officials who routinely participate in the State or major urban area's homeland security preparedness activities.

It is important to stress that this *behavior-focused approach* to identifying suspicious activity requires that factors such as race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (except if used as part of a specific suspect description). It is also important to recognize that many terrorism activities are now being funded via local or regional criminal organizations whose direct association with terrorism may be tenuous. This places law enforcement and homeland security professionals in the unique, yet demanding, position of identifying suspicious activities or materials as a byproduct or secondary element in a criminal enforcement or investigation activity. This means that, while some ISE-SARs may document activities or incidents to which local agencies have already responded, there is value in sharing them more broadly to facilitate aggregate trending or analysis.

Suspicious Activity Reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory operations although they can provide information to these activities. The ISE-SAR effort offers a standardized means for sharing information regarding behavior potentially related to terrorism-related criminal activity and applying data analysis tools to the information. Any patterns identified during ISE-SAR data analysis may be investigated in cooperation with the reporting agency, Joint Terrorism Task Force (JTTF), or the State or major urban area fusion center in accordance with departmental policies and procedures. Moreover, the same constitutional standards that apply when conducting ordinary criminal investigations also apply to local law enforcement and homeland security officers conducting SAR inquiries. This means, for example, that constitutional protections and agency policies and procedures that apply to a law enforcement officer's authority to stop, stop and frisk ("Terry Stop")⁴, request identification, or detain and question an individual would apply in the same measure whether or not the observed behavior related to terrorism or any other criminal activity.

C. Overview of Nationwide SAR Cycle

As defined in the *Nationwide Suspicious Activity Reporting Initiative (NSI) Concept of Operations (CONOPS)*⁵ and shown in Figure 1, the nationwide SAR process involves a total of 12 discrete steps that are grouped under five standardized business process activities – Planning, Gathering and Processing, Analysis and Production, Dissemination, and Reevaluation. The top-level ISE-SAR business process described in this section has been revised to be consistent with the description in the *NSI CONOPS*. Consequently, the numbered steps in Figure 1 are the only ones that map directly to the nine-steps of the detailed information flow for nationwide SAR information sharing documented in Part C of this version of the *ISE-SAR Functional Standard*. For further detail on the 12 NSI steps, please refer to the *NSI CONOPS*.

⁴ "Terry Stop" refers to law enforcement circumstances related to Supreme Court of the United States ruling on "Terry v. Ohio (No. 67)" argued on December 12, 1967 and decided on June 10, 1968. This case allows a law enforcement officer to articulate reasonable suspicion as a result of a totality of circumstances (to include training and experience) and take action to frisk an individual for weapons that may endanger the officer. The Opinion of the Supreme Court regarding this case may be found at Internet site http://www.law.cornell.edu/supct/html/historics/USSC_CR_0392_0001_ZO.html.

⁵ PM-ISE, *Nationwide SAR Initiative Concept of Operations* (Washington: PM-ISE, 2008), available from www.ise.gov.

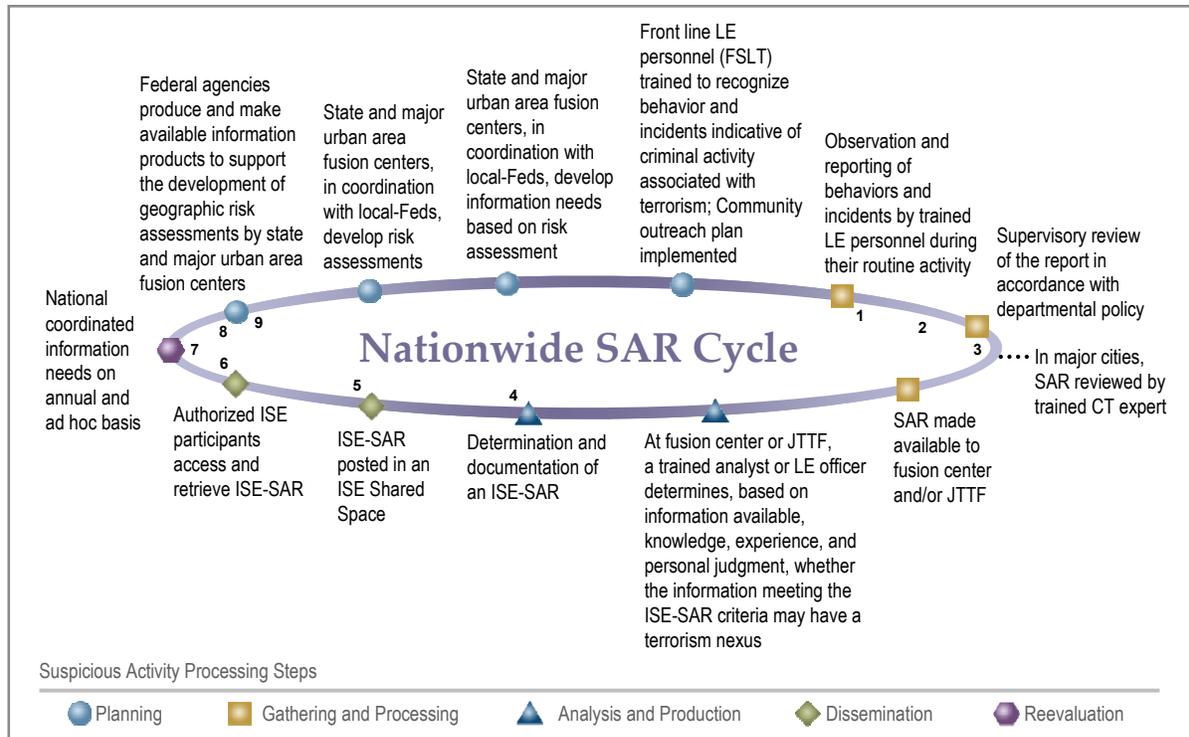


Figure 1. Overview of Nationwide SAR Process

D. ISE-SAR Top-Level Business Process

1. Planning

The activities in the planning phase of the NSI cycle, while integral to the overall NSI, are not discussed further in this Functional Standard. See the NSI CONOPS for more details.⁶

2. Gathering and Processing

Local law enforcement agencies or field elements of Federal agencies gather and document suspicious activity information in support of their responsibilities to investigate potential criminal activity, protect citizens, apprehend and prosecute criminals, and prevent crime. Information acquisition begins with an observation or report of unusual or suspicious behavior that may be indicative of criminal activity associated with terrorism. Such activities include, but are not limited to, theft, loss, or diversion, site breach or physical intrusion, cyber attacks, possible testing of physical response, or other unusual behavior or sector specific incidents. It is important to emphasize that context is an essential element of interpreting the relevance of such behaviors to criminal activity associated with terrorism. (See Part B for more details.)

⁶ Ibid., 17-18.

Regardless of whether the initial observer is a private citizen, a representative of a private sector partner, a government official, or a law enforcement officer, suspicious activity is eventually reported to either a local law enforcement agency or a local, regional, or national office of a Federal agency. When the initial investigation or fact gathering is completed, the investigating official documents the event in accordance with agency policy, local ordinances, and State and Federal laws and regulations.

The information is reviewed within a local or Federal agency by appropriately designated officials for linkages to other suspicious or criminal activity in accordance with departmental policy and procedures.⁷ Although there is always some level of local review, the degree varies from agency to agency. Smaller agencies may forward most SARs directly to the State or major urban area fusion center or JTTF with minimal local processing. Major cities, on the other hand, may have trained counterterrorism experts on staff that apply a more rigorous analytic review of the initial reports and filter out those that can be determined not to have a potential terrorism nexus.

After appropriate local processing, agencies make SARs available to the relevant State or major urban area fusion center. Field components of Federal agencies forward their reports to the appropriate regional, district, or headquarters office employing processes that vary from agency to agency. Depending on the nature of the activity, the information could cross the threshold of “suspicious” and move immediately into law enforcement operations channels for follow-on action against the identified terrorist activity. In those cases where the local agency can determine that an activity has a direct connection to criminal activity associated with terrorism, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation of a terrorism-related crime as appropriate.

3. Analysis and Production

The fusion center or Federal agency enters the SAR into its local information system and then performs an additional analytic review to establish or discount a potential terrorism nexus. First, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR criteria outlined in Part B of this *ISE-SAR Functional Standard*. Second, the Terrorist Screening Center (TSC) should be contacted to determine if there is valuable information in the Terrorist Screening Database. Third, he or she will review the input against all available knowledge and information for linkages to other suspicious or criminal activity.

Based on this review, the officer or analyst will apply his or her professional judgment to determine whether the information has a potential nexus to terrorism. If the officer or analyst cannot make this explicit determination, the report will not be accessible by the ISE, although

⁷ If appropriate, the agency may consult with a Joint Terrorism Task Force, Field Intelligence Group, or fusion center.

it may be retained in local fusion center or Federal agency files in accordance with established retention policies and business rules.⁸

4. Dissemination

Once the determination of a potential terrorism nexus is made, the information becomes an ISE-SAR and is formatted in accordance with the ISE-SAR Information Exchange Package Document (IEPD) format described in Sections III and IV. This ISE-SAR is then stored in the fusion center, JTTF, or other Federal agency's ISE Shared Space⁹ where it can be accessed by authorized law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility as well as other ISE participants, including JTTFs. This allows the fusion center to be cognizant of all terrorist-related suspicious activity in its area of responsibility, consistent with the information flow description in Part C. Although the information in ISE Shared Spaces is accessible by other ISE participants, it remains under the control of the submitting organization, i.e., the fusion center or Federal agency that made the initial determination that the activity constituted an ISE-SAR.

By this stage of the process, all initially reported SARs have been through multiple levels of review by trained personnel and, to the maximum extent possible, those reports without a potential terrorism nexus have been filtered out. Those reports posted in ISE Shared Spaces, therefore, can be presumed by Federal, State, and local analytic personnel to be terrorism-related and information derived from them can be used along with other sources to support counterterrorism operations or develop counterterrorism analytic products. As in any analytic process, however, all information is subject to further review and validation, and analysts must coordinate with the submitting organization to ensure that the information is still valid and obtain any available relevant supplementary material before incorporating it into an analytic product.

Once ISE-SARs are accessible, they can be used to support a range of counterterrorism analytic and operational activities. This step involves the actions necessary to integrate ISE-SAR information into existing counterterrorism analytic and operational processes, including efforts to "connect the dots," identify information gaps, and develop formal analytic products. Depending on privacy policy and procedures established for the NSI as a whole or by agencies responsible for individual ISE Shared Spaces, requestors may only be able to view reports in the Summary ISE-SAR Information format, i.e., without privacy fields. In these cases, requestors should contact the submitting organization directly to discuss the particular report more fully and obtain access, where appropriate, to the information in the privacy fields.

⁸ As was already noted in the discussion of processing by local agencies, where the fusion center or Federal agency can determine that an activity has a direct connection to a possible terrorism-related crime, it will provide the information directly to the responsible JTTF for use as the basis for an assessment or investigation.

⁹ PM-ISE, *ISE Enterprise Architecture Framework, Version 2.0*, (Washington: PM-ISE, 2008), 61-63

5. Reevaluation¹⁰

Operational feedback on the status of ISE-SARs is an essential element of an effective NSI process with important implications for privacy and civil liberties. First of all, it is important to notify source organizations when information they provide is designated as an ISE-SAR by a submitting organization and made available for sharing—a form of positive feedback that lets organizations know that their initial suspicions have some validity. Moreover, the process must support notification of all ISE participants when further evidence determines that an ISE-SAR was designated incorrectly so that the original information does not continue to be used as the basis for analysis or action. This type of feedback can support organizational redress processes and procedures where appropriate.

E. Broader ISE-SAR Applicability

Consistent with the ISE Privacy Guidelines and Presidential Guideline 2, and to the full extent permitted by law, this *ISE-SAR Functional Standard* is designed to support the sharing of unclassified information or sensitive but unclassified (SBU)/controlled unclassified information (CUI) within the ISE. There is also a provision for using a data element indicator for designating classified national security information as part of the ISE-SAR record, as necessary. This condition could be required under special circumstances for protecting the context of the event, or specifics or organizational associations of affected locations. The State or major urban area fusion center shall act as the key conduit between the State, local, and tribal (SLT) agencies and other ISE participants. It is also important to note that the ISE Shared Spaces implementation concept is focused exclusively on terrorism-related information. However many SAR originators and consumers have responsibilities beyond terrorist activities. Of special note, there is no intention to modify or otherwise affect, through this *ISE-SAR Functional Standard*, the currently supported or mandated direct interactions between State, local, and tribal law enforcement and investigatory personnel and the Joint Terrorism Task Forces (JTTFs) or Field Intelligence Groups (FIGs).

This *ISE-SAR Functional Standard* will be used as the ISE-SAR information exchange standard for all ISE participants. Although the extensibility of this *ISE-SAR Functional Standard* does support customization for unique communities, jurisdictions planning to modify this *ISE-SAR Functional Standard* must carefully consider the consequences of customization. The PM-ISE requests that modification follow a formal change request process through the ISE-SAR Steering Committee and CTISS Committee under the Information Sharing Council, for both community coordination and consideration. Furthermore, messages that do not conform to this Functional Standard may not be consumable by the receiving organization and may require modifications by the nonconforming organizations.

¹⁰ The Reevaluation Phase also encompasses the establishment of an integrated counterterrorism information needs process, a process that does not relate directly to information exchanges through this standard. See page 23 of the *NSI CONOPS* for more details.

F. Protecting Privacy

Laws that prohibit or otherwise limit the sharing of personal information vary considerably between the Federal, State, local, and tribal levels. The Privacy Act of 1974 (5 USC §552a) as amended, other statutes such as the E-Government Act, and many government-wide or departmental regulations establish a framework and criteria for protecting information privacy in the Federal Government. The ISE must facilitate the sharing of information in a lawful manner, which by its nature must recognize, in addition to Federal statutes and regulations, different State, local or tribal laws, regulations, or policies that affect privacy. One method for protecting privacy while enabling the broadest possible sharing is to anonymize ISE-SAR reports by excluding data elements that contain personal information. Accordingly, two different formats are available for ISE-SAR information. The **Detailed ISE-SAR IEPD** format includes personal information contained in the data fields set forth in Section IV of this *ISE-SAR Functional Standard* (“ISE-SAR Exchange Data Model”), including “privacy fields” denoted as containing personal information. If an ISE participant is not authorized to disseminate personal information from an ISE Shared Space (e.g., the requester site does not have a compliant privacy policy) or the SAR does not evidence the necessary nexus to terrorism-related crime (as required by this *ISE-SAR Functional Standard*), information from the privacy fields will not be loaded into the responsive document (search results) from the ISE Shared Space. This personal information will not be passed to the ISE participant. The **Summary ISE-SAR Information** format excludes privacy fields or data elements identified in Section IV of this *ISE-SAR Functional Standard* as containing personal information. Each ISE participant can exclude additional data elements from the **Summary ISE-SAR Information** format in accordance with its own legal and policy requirements. It is believed the data contained within a **Summary ISE-SAR Information** format will support sufficient trending and pattern recognition to trigger further analysis and/or investigation where additional information can be requested from the sending organization. Because of variances of data expected within ISE-SAR exchanges, only the minimum elements are considered mandatory. These are enumerated in the READ ME document in the technical artifacts folder that is part of this *ISE-SAR Functional Standard*.

Currently, the privacy fields identified in the ISE-SAR exchange data model (Section IV, below) are the minimum fields that should be removed from a **Detailed ISE-SAR IEPD**.

SECTION III – INFORMATION EXCHANGE DEVELOPMENT

This *ISE-SAR Functional Standard* is a collection of artifacts that support an implementer’s creation of ISE-SAR information exchanges, whether **Detailed ISE-SAR IEPD** or **Summary ISE-SAR Information**. The basic ISE-SAR information exchange is documented using five unique artifacts giving implementers tangible products that can be leveraged for local implementation. A domain model provides a graphical depiction of those data elements required for implementing an exchange and the cardinality between those data elements. Second, a Component Mapping Template is a spreadsheet that associates each required data element with its corresponding XML data element. Third, information exchanges include the schemas which consist of a document, extension, and constraint schema. Fourth, at least one sample XML Instance and associated style-sheet is included to help practitioners validate the model, mapping,

and schemas in a more intuitive way. Fifth, a codified data field values listing provides listings, descriptions, and sources as prescribed by the data fields.

SECTION IV – ISE-SAR EXCHANGE DATA MODEL

A. Summary of Elements

This section contains a full inventory of all ISE-SAR information exchange data classes, elements, and definitions. Items and definitions contained in cells with a light purple background are data classes, while items and definition contained in cells with a white background are data elements. A wider representation of data class and element mappings to source (ISE-SAR information exchange) and target is contained in the Component Mapping Template located in the technical artifacts folder.

Cardinality between objects in the model is indicated on the line in the domain model (see Section 5A). Cardinality indicates how many times an entity can occur in the model. For example, Vehicle, Vessel, and Aircraft all have cardinality of 0..n. This means that they are optional, but may occur multiple times if multiple suspect vehicles are identified.

Clarification of Organizations used in the exchange:

- The **Source Organization** is the agency or entity that originates the SAR report (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The Source Organization will not change throughout the life of the SAR.
- The **Submitting Organization** is the organization providing the ISE-SAR to the community through their ISE Shared Space. The Submitting Organization and the Source Organization may be the same.
- The **Owning Organization** is the organization that owns the target associated with the suspicious activity.

Table 2 – ISE-SAR Information Exchange Data Classes, Elements, and Definitions

Privacy Field	Source Class/Element	Source Definition
	Aircraft	
	Aircraft Engine Quantity	The number of engines on an observed aircraft.
	Aircraft Fuselage Color	A code identifying a color of a fuselage of an aircraft.
	Aircraft Wing Color	A code identifying a color of a wing of an aircraft.
X	Aircraft ID	A unique identifier assigned to the aircraft by the observing organization—used for referencing. *If this identifier can be used to identify a specific aircraft, for instance, by using the aircraft tail number, then this element is a privacy field. [free text field]
	Aircraft Make Code	A code identifying a manufacturer of an aircraft.
	Aircraft Model Code	A code identifying a specific design or type of aircraft made by a manufacturer.

Privacy Field	Source Class/Element	Source Definition
	Aircraft Style Code	A code identifying a style of an aircraft.
X	Aircraft Tail Number	An aircraft identification number prominently displayed at various locations on an aircraft, such as on the tail and along the fuselage. [free text field]
	Attachment	
	Attachment Type Text	Describes the type of attachment (e.g., surveillance video, mug shot, evidence). [free text field]
	Binary Image	Binary encoding of the attachment.
	Capture Date	The date that the attachment was created.
	Description Text	Text description of the attachment. [free text field]
	Format Type Text	Format of attachment (e.g., mpeg, jpg, avi). [free text field]
	Attachment URI	Uniform Resource Identifier (URI) for the attachment. Used to match the attachment link to the attachment itself. Standard representation type that can be used for Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).
	Attachment Privacy Field Indicator	Identifies whether the binary attachment contains information that may be used to identify an individual.
	Contact Information	
	Person First Name	Person to contact at the organization.
	Person Last Name	Person to contact at the organization.
	E-Mail Address	An email address of a person or organization. [free text field]
	Full Telephone Number	A full length telephone identifier representing the digits to be dialed to reach a specific telephone instrument. [free text field]
	Driver License	
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Authority Text	Code identifying the organization that issued the driver license assigned to the person. Examples include Department of Motor Vehicles, Department of Public Safety and Department of Highway Safety and Motor Vehicles. [free text field]
X	Driver License Number	A driver license identifier or driver license permit identifier of the observer or observed person of interest involved with the suspicious activity. [free text field]
	Follow-Up Action	
	Activity Date	Date that the follow-up activity started.
	Activity Time	Time that the follow up activity started.
	Assigned By Text	Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations. [free text field]
	Assigned To Text	Text describing the person or sub-organization that will be performing the designated action. [free text field]
	Disposition Text	Description of disposition of suspicious activity investigation. [free text field]
	Status Text	Description of the state of follow-up activity. [free text field]
	Location	

Privacy Field	Source Class/Element	Source Definition
X	Location Description	A description of a location where the suspicious activity occurred. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Location Address	
	Building Description	A complete reference that identifies a building. [free text field]
	County Name	A name of a county, parish, or vicinage. [free text field]
	Country Name	A country name or other identifier. [free text field]
	Cross Street Description	A description of an intersecting street. [free text field]
	Floor Identifier	A reference that identifies an actual level within a building. [free text field]
	ICAO Airfield Code for Departure	An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information. [free text field]
	ICAO Airfield Code for Planned Destination	An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information [free text field]
	ICAO for Actual Destination	An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	ICAO Airfield for Alternate	An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information. [free text field]
	Mile Marker Text	Identifies the sequentially numbered marker on a roadside that is closest to the intended location. Also known as milepost, or mile post. [free text field]
	Municipality Name	The name of the city or town. [free text field]
	Postal Code	The zip code or postal code. [free text field]
	State Name	Code identifying the state.
	Street Name	A name that identifies a particular street. [free text field]
X	Street Number	A number that identifies a particular unit or location within a street. [free text field]
	Street Post Directional	A direction that appears after a street name. [free text field]
	Street Pre Directional	A direction that appears before a street name. [free text field]
	Street Type	A type of street, e.g., Street, Boulevard, Avenue, Highway. [free text field]
X	Unit ID	A particular unit within the location. [free text field]
	Location Coordinates	
	Altitude	Height above or below sea-level of a location.
	Coordinate Datum	Coordinate system used for plotting location.
	Latitude Degree	A value that specifies the degree of a latitude. The value comes from a restricted range between -90 (inclusive) and +90 (inclusive).
	Latitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Latitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).

Privacy Field	Source Class/Element	Source Definition
	Longitude Degree	A value that specifies the degree of a longitude. The value comes from a restricted range between -180 (inclusive) and +180 (exclusive).
	Longitude Minute	A value that specifies a minute of a degree. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Longitude Second	A value that specifies a second of a minute. The value comes from a restricted range of 0 (inclusive) to 60 (exclusive).
	Conveyance track/intent	A direction by heading and speed or enroute route and/or waypoint of conveyance [free text field]
	Observer	
	Observer Type Text	Indicates the relative expertise of an observer to the suspicious activity (e.g., professional observer versus layman). Example: a security guard at a utility plant recording the activity, or a citizen driving by viewing suspicious activity. [free text field]
X	Person Employer ID	Number assigned by an employer for a person such as badge number. [free text field]
	Owning Organization	
	Organization Item	A name of an organization that owns the target. [free text field]
	Organization Description	A text description of organization that owns the target. The description may indicate the type of organization such as State Bureau of Investigation, Highway Patrol, etc. [free text field]
X	Organization ID	A federal tax identifier assigned to an organization. Sometimes referred to as a Federal Employer Identification Number (FEIN), or an Employer Identification Number (EIN). [free text field]
	Organization Local ID	An identifier assigned on a local level to an organization. [free text field]
	Other Identifier	
X	Person Identification Number (PID)	An identifying number assigned to the person, e.g., military serial numbers. [free text field]
X	PID Effective Date	The month, date, and year that the PID number became active or accurate.
	PID Effective Year	The year that the PID number became active or accurate.
X	PID Expiration Date	The month, date, and year that the PID number expires.
	PID Expiration Year	The year that the PID number expires.
	PID Issuing Authority Text	The issuing authority of the identifier. This may be a State, military organization, etc.
	PID Type Code	Code identifying the type of identifier assigned to the person. [free text field]
	Passport	
X	Passport ID	Document Unique Identifier. [free text field]
X	Expiration Date	The month, date, and year that the document expires.
	Expiration Year	The year the document expires.
	Issuing Country Code	Code identifying the issuing country. [free text field]
	Person	
X	AFIS FBI Number	A number issued by the FBI's Automated Fingerprint Identification System (AFIS) based on submitted fingerprints. [free text field]

Privacy Field	Source Class/Element	Source Definition
	Age	A precise measurement of the age of a person.
	Age Unit Code	Code that identifies the unit of measure of an age of a person (e.g., years, months). [free text field]
X	Date of Birth	The month, date, and year that a person was born.
	Year of Birth	The year a person was born.
	Ethnicity Code	Code that identifies the person's cultural lineage.
	Maximum Age	The maximum age measurement in an estimated range.
	Minimum Age	The minimum age measurement in an estimated range.
X	State Identifier	Number assigned by the State based on biometric identifiers or other matching algorithms. [free text field]
X	Tax Identifier Number	A 9-digit numeric identifier assigned to a living person by the U.S. Social Security Administration. A social security number of the person. [free text field]
	Person Name	
X	First Name	A first name or given name of the person. [free text field]
X	Last Name	A last name or family name of the person. [free text field]
X	Middle Name	A middle name of a person. [free text field]
X	Full Name	Used to designate the compound name of a person that includes all name parts. This field should only be used when the name cannot be broken down into its component parts or if the information is not available in its component parts. [free text field]
X	Moniker	Alternative, or gang name for a person. [free text field]
	Name Suffix	A component that is appended after the family name that distinguishes members of a family with the same given, middle, and last name, or otherwise qualifies the name. [free text field]
	Name Type	Text identifying the type of name for the person. For example, maiden name, professional name, nick name.
	Physical Descriptors	
	Build Description	Text describing the physique or shape of a person. [free text field]
	Eye Color Code	Code identifying the color of the person's eyes.
	Eye Color Text	Text describing the color of a person's eyes. [free text field]
	Hair Color Code	Code identifying the color of the person's hair.
	Hair Color Text	Text describing the color of a person's hair. [free text field]
	Person Eyewear Text	A description of glasses or other eyewear a person wears. [free text field]
	Person Facial Hair Text	A kind of facial hair of a person. [free text field]
	Person Height	A measurement of the height of a person.
	Person Height Unit Code	Code that identifies the unit of measure of a height of a person. [free text field]
	Person Maximum Height	The maximum measure value on an estimated range of the height of the person.
	Person Minimum Height	The minimum measure value on an estimated range of the height of the person.
	Person Maximum Weight	The maximum measure value on an estimated range of the weight of the person.

Privacy Field	Source Class/Element	Source Definition
	Person Minimum Weight	The minimum measure value on an estimated range of the weight of the person.
	Person Sex Code	A code identifying the gender or sex of a person (e.g., Male or Female).
	Person Weight	A measurement of the weight of a person.
	Person Weight Unit Code	Code that identifies the unit of measure of a weight of a person. [free text field]
	Race Code	Code that identifies the race of the person.
	Skin Tone Code	Code identifying the color or tone of a person's skin.
	Clothing Description Text	A description of an article of clothing. [free text field]
	Physical Feature	
	Feature Description	A text description of a physical feature of the person. [free text field]
	Feature Type Code	A special kind of physical feature or any distinguishing feature. Examples include scars, marks, tattoos, or a missing ear. [free text field]
	Location Description	A description of a location. If the location is an address that is not broken into its component parts (e.g., 1234 Main Street), this field may be used to store the compound address. [free text field]
	Registration	
	Registration Authority Code	Text describing the organization or entity authorizing the issuance of a registration for the vehicle involved with the suspicious activity. [free text field]
X	Registration Number	The number on a metal plate fixed to/assigned to a vehicle. The purpose of the registration number is to uniquely identify each vehicle within a state. [free text field]
	Registration Type	Code that identifies the type of registration plate or license plate of a vehicle. [free text field]
	Registration Year	A 4-digit year as shown on the registration decal issued for the vehicle.
	ISE-SAR Submission	
	Additional Details Indicator	Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.
	Data Entry Date	Date the data was entered into the reporting system (e.g., the Records Management System).
	Dissemination Code	Generally established locally, this code describes the authorized recipients of the data. Examples include Law Enforcement Use, Do Not Disseminate, etc.
	Fusion Center Contact First Name	Identifies the first name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Last Name	Identifies the last name of the person to contact at the fusion center. [free text field]
	Fusion Center Contact E-Mail Address	Identifies the email address of the person to contact at the fusion center. [free text field]
	Fusion Center Contact Telephone Number	The full phone number of the person at the fusion center that is familiar with the record (e.g., law enforcement officer).

Privacy Field	Source Class/Element	Source Definition
	Message Type Indicator	e.g., Add, Update, Purge.
	Privacy Purge Date	The date by which the privacy information will be purged from the record system; general observation data is retained.
	Privacy Purge Review Date	Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.
	Submitting ISE-SAR Record ID	Identifies the Fusion Center ISE-SAR Record identifier for reports that are possibly related to the current report. [free text field]
	ISE-SAR Submission Date	Date of submission for the ISE-SAR Record.
	ISE-SAR Title	Plain language title (e.g., Bomb threat at the "X" Hotel). [free text field]
	ISE-SAR Version	Indicates the specific version of the ISE-SAR that the XML Instance corresponds. [free text field]
	Source Agency Case ID	The case identifier for the agency that originated the SAR. Often, this will be a local law enforcement agency. [free text field]
	Source Agency Record Reference Name	The case identifier that is commonly used by the source agency—may be the same as the System ID. [free text field]
	Source Agency Record Status Code	The current status of the record within the source agency system.
	Privacy Information Exists Indicator	Indicates whether privacy information is available from the source fusion center. This indicator may be used to guide people who only have access to the summary information exchange as to whether or not they can follow-up with the originating fusion center to obtain more information.
	Sensitive Information Details	
	Classification Label	A classification of information. Includes Confidential, Secret, Top Secret, no markings. [free text field]
	Classification Reason Text	A reason why the classification was made as such. [free text field]
	Sensitivity Level	Local information security categorization level (Controlled Unclassified Information-CUI, including Sensitive But Unclassified or Law Enforcement Sensitive). [free text field]
	Tearlined Indicator	Identifies whether a report is free of classified information.
	Source Organization	
	Organization Name	The name used to refer to the agency originating the SAR. [free text field]
	Organization ORI	Originating Agency Identification (ORI) used to refer to the agency.
	System ID	The system that the case identifier (e.g., Records Management System, Computer Aided Dispatch) relates to within or the organization that originated the Suspicious Activity Report. [free text field]
	Fusion Center Submission Date	Date of submission to the Fusion Center.
	Source Agency Contact First Name	The first name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Last Name	The last name of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]
	Source Agency Contact Email Address	The email address of the person at the agency that is familiar with the record (e.g., law enforcement officer). [free text field]

Privacy Field	Source Class/Element	Source Definition
	Source Agency Contact Phone Number	The full phone number of the person at the agency that is familiar with the record (e.g., law enforcement officer).
	Suspicious Activity Report	
	Community Description	Describes the intended audience of the document. [free text field]
	Community URI	The URL to resolve the ISE-SAR information exchange payload namespace.
	LEXS Version	Identifies the version of Department of Justice LEISP Exchange Specification (LEXS) used to publish this document. ISE-FS-200 has been built using LEXS version 3.1. The schema was developed by starting with the basic LEXS schema and extending that definition by adding those elements not included in LEXS. [free text field]
	Message Date/Time	A timestamp identifying when this message was received.
	Sequence Number	A number that uniquely identifies this message.
	Source Reliability Code	Reliability of the source, in the assessment of the reporting organization: could be one of 'reliable', 'unreliable', or 'unknown'
	Content Validity Code	Validity of the content, in the assessment of the reporting organization: could be one of 'confirmed', 'doubtful', or 'cannot be judged'
	Nature of Source-Code	Nature of the source: Could be one of 'anonymous tip', 'confidential source', trained interviewer', 'written statement – victim, witness, other', private sector', or 'other source'
	Nature of Source-Text	Optional information of 'other source' is selected above. [free text field]
	Submitting Organization	
	Organization Name	Common Name of the fusion center or ISE participant that submitted the ISE-SAR record to the ISE. [free text field]
	Organization ID	Fusion center or ISE participant's alpha-numeric identifier. [free text field]
	Organization ORI	ORI for the submitting fusion center or ISE participant. [free text field]
	System ID	Identifies the system within the fusion center or ISE participant that is submitting the ISE-SAR. [free text field]
	Suspicious Activity	
	Activity End Date	The end or completion date in Greenwich Mean Time (GMT) of an incident that occurs over a duration of time.
	Activity End Time	The end or completion time in GMT of day of an incident that occurs over a duration of time.
	Activity Start Date	The date in GMT when the incident occurred or the start date if the incident occurs over a period of time.
	Activity Start Time	The time of day in GMT that the incident occurred or started.
	Observation Description Text	Description of the activity including rational for potential terrorism nexus. [free text field]
	Observation End Date	The end or completion date in GMT of the observation of an activity that occurs over a duration of time.
	Observation End Time	The end or completion time of day in GMT of the observation of an activity that occurred over a period of time.

Privacy Field	Source Class/Element	Source Definition
	Observation Start Date	The date in GMT when the observation of an activity occurred or the start date if the observation of the activity occurred over a period of time.
	Observation Start Time	The time of day in GMT that the observation of an activity occurred or started.
	Threat Type Code	Broad category of threat to which the tip or lead pertains. Includes Financial Incident, Suspicious Activity, and Cyber Crime.
	Threat Type Detail Text	Breakdown of the Tip Type, it indicates the type of threat to which the tip or lead pertains. The subtype is often dependent on the Tip Type. For example, the subtypes for a nuclear/radiological tip class might be Nuclear Explosive or a Radiological Dispersal Device. [free text field]
	Suspicious Activity Code	Indicates the type of threat to which the tip or lead pertains. Examples include a biological or chemical threat.
	Weather Condition Details	The weather at the time of the suspicious activity. The weather may be described using codified lists or text.
	Target	
	Critical Infrastructure Indicator	Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
	Infrastructure Sector Code	The broad categorization of the infrastructure type. These include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.
	Infrastructure Tier Text	Provides additional detail that enhances the Target Sector Code. For example, if the target sector is Utilities, this field would indicate the type of utility that has been targeted such as power station or power transmission. [free text field]
	Structure Type Code	National Data Exchange (N-DEX) Code that identifies the type of Structure that was involved in the incident.
	Target Type Text	Describes the target type if an appropriate sector code is not available. [free text field]
	Structure Type Text	Text for use when the Structure Type Code does not afford necessary code. [free text field]
	Target Description Text	Text describing the target (e.g., Lincoln Bridge). [free text field]
	Vehicle	
	Color Code	Code that identifies the primary color of a vehicle involved in the suspicious activity.
	Description	Text description of the entity. [free text field]
	Make Name	Code that identifies the manufacturer of the vehicle.
	Model Name	Code that identifies the specific design or type of vehicle made by a manufacturer—sometimes referred to as the series model.
	Style Code	Code that identifies the style of a vehicle. [free text field]
	Vehicle Year	A 4-digit year that is assigned to a vehicle by the manufacturer.

Privacy Field	Source Class/Element	Source Definition
X	Vehicle Identification Number	Used to uniquely identify motor vehicles. [free text field]
X	US DOT Number	An assigned number sequence required by Federal Motor Carrier Safety Administration (FMCSA) for all interstate carriers. The identification number (found on the power unit, and assigned by the U.S. Department of Transportation or by a State) is a key element in the FMCSA databases for both carrier safety and regulatory purposes. [free text field]
	Vehicle Description	A text description of a vehicle. Can capture unique identifying information about a vehicle such as damage, custom paint, etc. [free text field]
	Related ISE-SAR	
	Fusion Center ID	Identifies the fusion center that is the source of the ISE-SAR. [free text field]
	Fusion Center ISE-SAR Record ID	Identifies the fusion center ISE-SAR record identifier for reports that are possibly related to the current report.
	Relationship Description Text	Describes how this ISE-SAR is related to another ISE-SAR. [free text field]
	Vessel	
X	Vessel Official Coast Guard Number Identification	An identification for the Official (U.S. Coast Guard Number of a vessel). Number is encompassed within valid marine documents and permanently marked on the main beam of a documented vessel. [free text field]
X	Vessel ID	A unique identifier assigned to the boat record by the agency—used for referencing. [free text field]
	Vessel ID Issuing Authority	Identifies the organization authorization over the issuance of a vessel identifier. Examples of this organization include the State Parks Department and the Fish and Wildlife department. [free text field]
X	Vessel IMO Number Identification	An identification for an International Maritime Organization Number (IMO number) of a vessel [free text field]
	Vessel MMSI Identification	An identification for the Maritime Mobile Service Identity (MMSI) or a vessel [free text field]
	Vessel Make	Code that identifies the manufacturer of the boat.
	Vessel Model	Model name that identifies the specific design or type of boat made by a manufacturer—sometimes referred to as the series model.
	Vessel Model Year	A 4-digit year that is assigned to a boat by the manufacturer.
	Vessel Name	Complete boat name and any numerics. [free text field]
	Vessel Hailing Port	The identifying attributes of the hailing port of a vessel [free text field]
	Vessel National Flag	A data concept for a country under which a vessel sails. [free text field]
	Vessel Overall Length	The length measurement of the boat, bow to stern.
	Vessel Overall Length Measure	Code that identifies the measurement unit used to determine the boat length. [free text field]
X	Vessel Serial Number	The identification number of a boat involved in an incident. [free text field]
	Vessel Type Code	Code that identifies the type of boat.

Privacy Field	Source Class/Element	Source Definition
	Vessel Propulsion Text	Text for use when the Boat Propulsion Code does not afford necessary code. [free text field]

B. Association Descriptions

This section defines specific data associations contained in the ISE-SAR data model structure. Reference Figure 2 (UML-based model) for the graphical depiction and detailed elements.

Table 3 – ISE-SAR Data Model Structure Associations

Link Between Associated Components	Target Element
Link From Suspicious Activity Report to Attachment	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityAttachmentLinkAssociation
Link From Suspicious Activity Report to Sensitive Information Details	Hierarchical Association
Link From Suspicious Activity Report to ISE-SAR Submission	Hierarchical Association
Link From Suspicious Activity to Vehicle	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Vehicle to Registration	Hierarchical Association
Link From Suspicious Activity to Vessel	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Aircraft	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentInvolvedItemAssociation
Link From Suspicious Activity to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ActivityLocationAssociation
Link From Suspicious Activity to Target	Hierarchical Association
Link From Location to Location Coordinates	Hierarchical Association
Link From Location to Location Address	Hierarchical Association
Link From Suspicious Activity Report to Related ISE-SAR	Hierarchical Association
Link From Person to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonLocationAssociation
Link From Person to Contact Information	lexs:Digest/lexsdigest:Associations/lexsdigest:EntityEmailAssociation or lexs:Digest/lexsdigest:Associations/lexsdigest:EntityTelephoneNumberAssociation
Link From Person to Driver License	Hierarchical Association
Link From Person to Passport	Hierarchical Association
Link From Person to Other Identifier	Hierarchical Association

Link Between Associated Components	Target Element
Link From Person to Physical Descriptors	Hierarchical Association
Link From Person to Physical Feature	Hierarchical Association
Link From Person to Person Name	Hierarchical Association
Link From Suspicious Activity Report to Follow-Up Action	Hierarchical Association
Link From Target to Location	lexs:Digest/lexsdigest:Associations/lexsdigest:ItemLocationAssociation
Link From Suspicious Activity Report to Organization	Hierarchical Association
Link From Suspicious Activity to Person [Witness]	lexs:Digest/lexsdigest:Associations/lexsdigest:IncidentWitnessAssociation
Link From Suspicious Activity to Person [Person Of Interest]	lexs:Digest/lexsdigest:Associations/lexsdigest:PersonOfInterestAssociation
Link From Organization to Target	ext:SuspiciousActivityReport/nc:OrganizationItemAssociation
Link from ISE-SAR Submission to Submitting Organization	Hierarchical Association
Link From Submitting Organization to Contact Information	Hierarchical Association (Note that the mapping indicates context and we are not reusing Contact Information components)

C. Extended XML Elements

Additional data elements are also identified as new elements outside of NIEM, Version 2.0. These elements are listed below:

AdditionalDetailsIndicator: Identifies whether more ISE-SAR details are available at the authoring/originating agency than what has been provided in the information exchange.

AssignedByText: Organizational identifier that describes the organization performing a follow-up activity. This is designed to keep all parties interested in a particular ISE-SAR informed of concurrent investigations.

AssignedToText: Text describing the person or sub-organization that will be performing the designated follow-up action.

ClassificationReasonText: A reason why the classification was made as such.

ContentValidityCode: Validity of the content, in the assessment of the reporting organization: could be one of 'confirmed', 'doubtful', or 'cannot be judged'.

ConveyanceTrack/intent: A direction by heading and speed or enroute route and/or waypoint of conveyance.

CriticalInfrastructureIndicator: Critical infrastructure, as defined by 42 USC Sec. 5195c, means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

ICAOAirfieldCodeforDeparture: An International Civil Aviation Organization (ICAO) airfield code for departure, indicates aircraft, crew, passengers, and cargo-on conveyance location information.

ICAOAirfieldCodeforPlannedDestination: An airfield code for planned destination, indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOforActualDestination: An airfield code for actual destination. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

ICAOAirfieldforAlternate: An airfield code for Alternate. Indicates aircraft, crew, passengers, and cargo on conveyance location information.

NatureofSource-Code: Nature of the source: Could be one of ‘anonymous tip’, ‘confidential source’, ‘trained interviewer’, ‘written statement – victim, witness, other’, ‘private sector’, or ‘other source’.

PrivacyFieldIndicator: Data element that may be used to identify an individual and therefore is subject to protection from disclosure under applicable privacy rules. Removal of privacy fields from a detailed report will result in a summary report. This privacy field informs users of the summary information exchange that additional information may be available from the originator of the report.

ReportPurgeDate: The date by which the privacy fields will be purged from the record system; general observation data is retained. Purge policies vary from jurisdiction to jurisdiction and should be indicated as part of the guidelines.

ReportPurgeReviewDate: Date of review to determine the disposition of the privacy fields in a Detailed ISE-SAR IEPD record.

SourceReliabilityCode: Reliability of the source, in the assessment of the reporting organization: could be one of ‘reliable’, ‘unreliable’, or ‘unknown’.

VesselHailingPort: The identifying attributes of the hailing port of a vessel.

VesselNationalFlag: A data concept for a country under which a vessel sails.

SECTION V – INFORMATION EXCHANGE IMPLEMENTATION ARTIFACTS

A. Domain Model

1. General Domain Model Overview

The domain model provides a visual representation of the business data requirements and relationships (Figure 2). This Unified Modeling Language (UML)-based Model represents the Exchange Model artifact required in the information exchange development methodology. The model is designed to demonstrate the organization of data elements and illustrate how these elements are grouped together into Classes. Furthermore, it describes relationships between these Classes. A key consideration in the development of a Domain Model is that it must be independent of the mechanism intended to implement the model. The domain model is actually a representation of how data is structured from a *business* context. As the technology changes and new Functional Standards emerge, developers can create new standards mapping documents and schema tied to a new standard without having to re-address business process requirements.

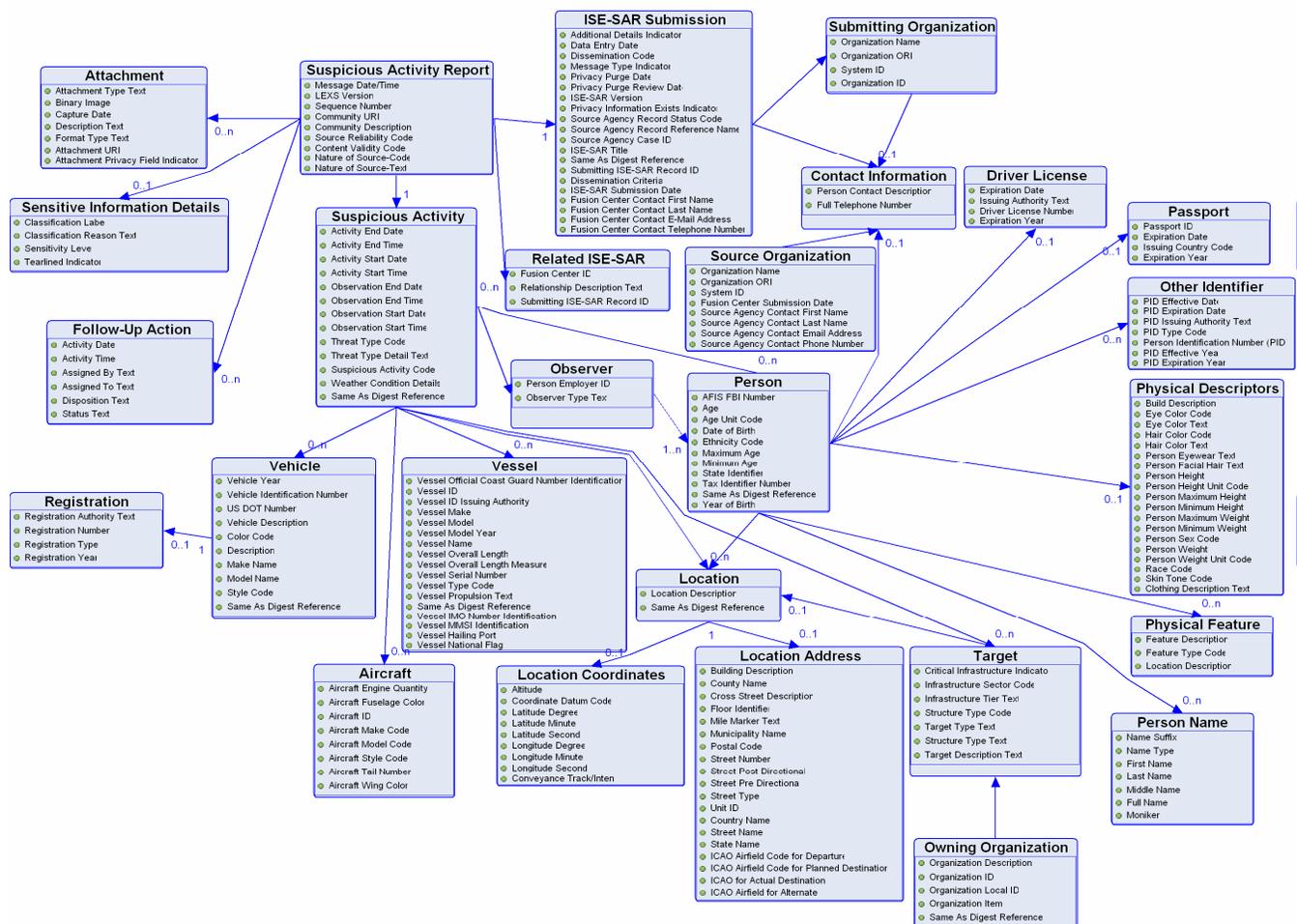


Figure 2 – UML-based Model

B. General Mapping Overview

The detailed component mapping template provides a mechanism to cross-reference the business data requirements documented in the Domain Model to their corresponding XML Element in the XML Schema. It includes a number of items to help establish equivalency including the business definition and the corresponding XML Element Definition.

C. ISE-SAR Mapping Overview

The Mapping Spreadsheet contains seven unique items for each ISE-SAR data class and element. The Mapping Spreadsheet columns are described in this section.

Table 4 – Mapping Spreadsheet Column Descriptions

Spreadsheet Name & Row	Description
Privacy Field Indicator	This field indicates that the information may be used to identify an individual.
Source Class/ Element	Content in this column is either the data class (grouping of data elements) or the actual data elements. Classes are highlighted and denoted with cells that contain blue background while elements have a white background. The word "Source" is referring to the ISE-SAR information exchange.
Source Definition	The content in this column is the class or element definition defined for this ISE-SAR information exchange. The word "Source" is referring to the ISE-SAR information exchange definition.
Target Element	The content in this column is the actual namespace path deemed equal to the related ISE-SAR information exchange element.
Target Element Definition	The content in this column provides the definition of the target or NIEM element located at the aforementioned source path. "Target" is referring to the NIEM definition.
Target Element Base	Indicates the data type of the terminal element. Data types of niem-xsd:String or nc:TextType indicate free-form text fields.
Mapping Comments	Provides technical implementation information for developers and implementers of the information exchange.

D. Schemas

The *ISE-SAR Functional Standard* contains the following compliant schemas;

- Subset Schema
- Exchange Schema
- Extension Schema
- Wantlist

E. Examples

The *ISE-SAR Functional Standard* contains two samples that illustrate exchange content as listed below.

1. XSL Style Sheet

This information exchange artifact provides an implementer and users with a communication tool which captures the look and feel of a familiar form, screen, or like peripheral medium for schema translation testing and user validation of business rules.

2. XML Instance

This information exchange artifact provides an actual payload of information with data content defined by the schema(s).

PART B – ISE-SAR CRITERIA GUIDANCE

Category	Description
DEFINED CRIMINAL ACTIVITY AND POTENTIAL TERRORISM NEXUS ACTIVITY	
Breach/Attempted Intrusion	Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).
Misrepresentation	Presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).
Sabotage/Tampering/Vandalism	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
Cyber Attack	Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
Aviation Activity	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.
POTENTIAL CRIMINAL OR NON-CRIMINAL ACTIVITY REQUIRING ADDITIONAL FACT INFORMATION DURING INVESTIGATION¹¹	
Eliciting Information	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
Recruiting	Building of operations teams and contacts, personnel data, banking data or travel data
Photography	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc.

11

Note: These activities are generally First Amendment-protected activities and should not be reported in a SAR or ISE-SAR absent articulable facts and circumstances that support the source agency's suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions).

Category	Description
Observation/Surveillance	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
Materials Acquisition/Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.
Acquisition of Expertise	Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
Weapons Discovery	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector), with regard to their personnel, facilities, systems or functions.

PART C – ISE-SAR INFORMATION FLOW DESCRIPTION

Step	Activity	Process	Notes
1	Observation	The information flow begins when a person observes behavior or activities that would appear suspicious to a reasonable person. Such activities could include, but are not limited to, expressed or implied threats, probing of security responses, site breach or physical intrusion, cyber attacks, indications of unusual public health sector activity, unauthorized attempts to obtain precursor chemical/agents or toxic materials, or other usual behavior or sector-specific incidents. ¹²	The observer may be a private citizen, a government official, or a law enforcement officer.

¹² Suspicious activity reporting (SAR) is official documentation of observed behavior that may be reasonably indicative of intelligence gathering and/or pre-operational planning related to terrorism or other criminal activity. ISE-SARs are a subset of all SARs that have been determined by an appropriate authority to have a potential nexus to terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Step	Activity	Process	Notes
2	Initial Response and Investigation	<p>An official of a Federal, State, local, or tribal agency with jurisdiction responds to the reported observation.¹³ This official gathers additional facts through personal observations, interviews, and other investigative activities. This may, at the discretion of the official, require further observation or engaging the subject in conversation. Additional information acquired from such limited investigative activity could then be used to determine whether to dismiss the activity as innocent or escalate to the next step of the process. In the context of priority information requirements, as provided by State and major urban area fusion centers, the officer/agent may use a number of information systems to continue the investigation. These systems provide the officer/agent with a more complete picture of the activity being investigated. Some examples of such systems and the information they may provide include:</p> <p>Department of Motor Vehicles provides drivers license and vehicle registration information; National Crime Information Center provides wants and warrants information, criminal history information and access to the Terrorist Screening Center and the terrorist watch list, Violent Gang/Terrorism Organization File (VGTOF), and Regional Information Sharing System (RISS); Other Federal, State, local, and tribal systems can provide criminal checks within the immediate and surrounding jurisdictions.</p> <p>When the initial investigation is complete, the official documents the event. The report becomes the initial record for the law enforcement or Federal agency's records management system (RMS).</p>	<p>The event may be documented using a variety of reporting mechanisms and processes, including but not limited to, reports of investigation, event histories, field interviews (FI), citations, incident reports, and arrest reports.</p> <p>The record may be hard and/or soft copy and does not yet constitute an ISE-SAR.</p>

¹³ If a suspicious activity has a direct connection to terrorist activity the flow moves along an operational path. Depending upon urgency, the information could move immediately into law enforcement operations and lead to action against the identified terrorist activity. In this case, the suspicious activity would travel from the initial law enforcement contact directly to the law enforcement agency with enforcement responsibility.

Step	Activity	Process	Notes
3	Local/Regional Processing	<p>The agency processes and stores the information in the RMS following agency policies and procedures. The flow will vary depending on whether the reporting organization is a State or local agency or a field element of a Federal agency.</p> <p>State, local, and tribal: Based on specific criteria or the nature of the activity observed, the State, local, and tribal law enforcement components forward the information to the State or major urban area fusion center for further analysis.</p> <p>Federal: Federal field components collecting suspicious activity would forward their reports to the appropriate resident, district, or division office. This information would be reported to field intelligence groups or headquarters elements through processes that vary from agency to agency.</p> <p>In addition to providing the information to its headquarters, the Federal field component would provide an information copy to the State or major urban area fusion center in its geographic region. This information contributes to the assessment of all suspicious activity in the State or major urban area fusion center's area of responsibility.</p>	<p>The State or major urban area fusion center should have access to all suspicious activity reporting in its geographic region whether collected by State, local, or tribal entities, or Federal field components.</p>
4	Creation of an ISE-SAR	<p>The determination of an ISE-SAR is a two-part process. First, at the State or major urban area fusion center or Federal agency, an analyst or law enforcement officer reviews the newly reported information against ISE-SAR behavior criteria. Second, based on available knowledge and information, the analyst or law enforcement officer determines whether the information meeting the criteria has a potential nexus to terrorism.</p> <p>Once this determination is made, the information becomes an "ISE-SAR" and is formatted in accordance with ISE-FS-200 (<i>ISE-SAR Functional Standard</i>). The ISE-SAR would then be shared with appropriate law enforcement and homeland security personnel in the State or major urban area fusion center's area of responsibility.</p>	<p>Some of this information may be used to develop criminal intelligence information or intelligence products which identifies trends and other terrorism related information and is derived from Federal agencies such as NCTC, DHS, and the FBI.</p> <p>For State, local, and tribal law enforcement, the ISE-SAR information may or may not meet the reasonable suspicion standard for criminal intelligence information. If it does, the information may also be submitted to a criminal intelligence information database and handled in accordance with 28 CFR Part 23.</p>

Step	Activity	Process	Notes
5	ISE-SAR Sharing and Dissemination	<p>In a State or major urban area fusion center, the ISE-SAR is shared with the appropriate FBI field components and the DHS representative and placed in the State or major urban area fusion center's ISE Shared Space or otherwise made available to members of the ISE.</p> <p>The FBI field component enters the ISE-SAR information into the FBI system and sends the information to FBI Headquarters.</p> <p>The DHS representative enters the ISE-SAR information into the DHS system and sends the information to DHS, Office of Intelligence Analysis.</p>	
6	Federal Headquarters (HQ) Processing	<p>At the Federal headquarters level, ISE-SAR information is combined with information from other State or major urban area fusion centers and Federal field components and incorporated into an agency-specific national threat assessment that is shared with ISE members.</p> <p>The ISE-SAR information may be provided to NCTC in the form of an agency-specific strategic threat assessment (e.g., strategic intelligence product).</p>	
7	NCTC Analysis	<p>When product(s) containing the ISE-SAR information are made available to NCTC, they are processed, collated, and analyzed with terrorism information from across the five communities—intelligence, defense, law enforcement, homeland security, and foreign affairs—and open sources.</p> <p>NCTC has the primary responsibility within the Federal government for analysis of terrorism information. NCTC produces federally coordinated analytic products that are shared through NCTC Online, the NCTC secure web site.</p> <p>The Interagency Threat Assessment and Coordinating Group (ITACG), housed at NCTC, facilitates the production of coordinated terrorism-related products that are focused on issues and needs of State, local, and tribal entities and when appropriate private sector entities. ITACG is the mechanism that facilitates the sharing of counterterrorism information with State, local, and tribal entities.</p>	

Step	Activity	Process	Notes
8	NCTC Alerts, Warnings, Notifications	NCTC products ¹⁴ , informed by the ITACG as appropriate, are shared with all appropriate Federal departments and agencies and with State, local, and tribal entities through the State or major urban area fusion centers. The sharing with State, local, and tribal entities and private sector occurs through the Federal departments or agencies that have been assigned the responsibility and have connectivity with the State or major urban area fusion centers. Some State or major urban area fusion centers, with secure connectivity and an NCTC Online account, can access NCTC products directly. State or major urban area fusion centers will use NCTC and ITACG informed products to help develop geographic-specific risk assessments (GSRA) to facilitate regional counterterrorism efforts. The GSRA are shared with State, local, and tribal entities and the private sector as appropriate. The recipient of the GSRA may use the GSRA to develop information gathering priorities or requirements.	NCTC products form the foundation of informational needs and guide collection of additional information. NCTC products should be responsive to informational needs of State, local, and tribal entities.
9	Focused Collection	The information has come full circle and the process begins again, informed by an NCTC or other Federal organization's product and the identified information needs of State, local and tribal entities and Federal field components.	

¹⁴ NCTC product include: Alerts, warnings, and notifications—identifying time sensitive or strategic threats; Situational awareness reports; and Strategic and foundational assessments of terrorist risks and threats to the United States and related intelligence information.

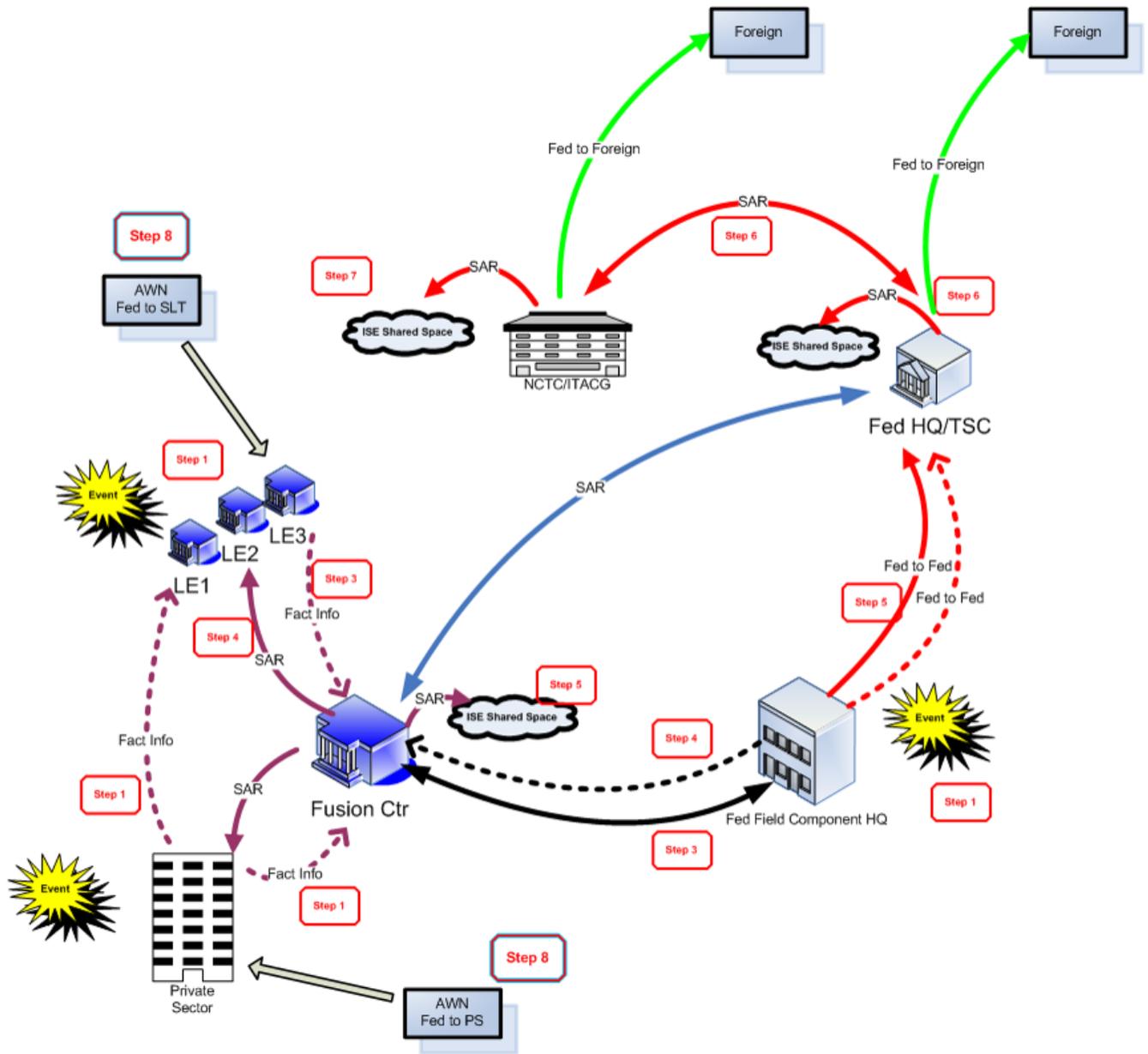


Figure 3 – SAR Information Flow Diagram

SJS Interface Specification

Revision	Date	Author	Changes
1.0	2002-05-13	NYS DCJS	Original
1.1	2004-01-12	NYSDCJS	<p>Added full arrest address instead of only CTV code. Added full crime location address instead of only CTV code.</p> <p>Note: The above changes were made to make the interface between SJS and IM stronger. This will have no impact on what is sent to DCJS but will greatly reduce the dual entry for officers.</p>
1.2	2006-02-01	NYSDCJS	<p>Addition of the following fields</p> <ol style="list-style-type: none"> 1. Condition at Arrest 2. CTV for home address 3. Home Phone 4. Residential Status 5. Marital Status 6. Education 7. Employment 8. Occupation 9. bail amount 10. search warrant 11. statement 12. warrant number 13. religion 14. *arrest for other agency info 15. Employer Information <p>All date formats are now yyyyddmm hh:mm:ss</p> <p>Photos returned by integration module will be stored in SJS for that arrest. File name must be 'mugshot.jpg' and located in the same directory as the record.xml file. Limit of size to 32k</p> <p>*When arresting for other agency The arrestingagency field will contain the arresting agency from the foa unless its an out of state manual entry in which case the arrestingagency will be the contributing agency.</p>
1.3	2007-05-23		<p>Addition of the following field:</p> <ol style="list-style-type: none"> 1. DIR Value of Y or N <p>Y – Yes Domestic Incident Report Filed – indicator is placed on Fingerprint Card.</p>

SJS Interface Specification

			N – No Domestic Incident Report filed. Indicator is blank on the fingerprint card
--	--	--	---

SJS Interface Specification

TABLE OF CONTENTS

1. Introduction	4
2. Business Flow	5
3. Operating System	5
4. File-Based Transfers	5
5. Directory Structure	6
6. Transactions	7
6.1 SJS TO INTEGRATION MODULE (IM)	7
6.2 INTEGRATION MODULE (IM) TO DCJS	7
6.3 DCJS TO INTEGRATION MODULE (IM)	8
6.4 INTEGRATION MODULE (IM) TO SJS	8
7. File Structure	8
APPENDIX A	8
APPENDIX B	14
APPENDIX C	19
APPENDIX D	20

SJS Interface Specification

1. Introduction

Spectrum Justice System (SJS) for Windows is an integrated law enforcement records management system developed and distributed by the New York State Division of Criminal Justice Services (DCJS). SJS was designed to help police officers perform their necessary functions including the processing and reporting of incident, arrest, and warrant records. Originally SJS was written for DOS and has been in the field for over 10 years. SJS DOS is installed in over 270 local police departments throughout the state. The redesign of the SJS DOS application, for the Windows architecture, was completed in 2001. An ongoing conversion of SJS DOS sites to the new Windows version continues, with expected completion by January 2003.

SJS was designed to help facilitate various reporting requirements. SJS can produce the standard incident report (SIR), the standard arrest report (SAR), warrant control sheet, arrest fingerprint cards for DCJS (adult and juvenile) and the FBI, and many other management reports. SJS provides the ability for the local agency to submit IBR, UCR (part I), and Crime mapping data, while maintaining data standards.

In the commitment by DCJS of federal and state resources to upgrading SJS to Windows, DCJS announced to the law enforcement community that SJS is the core product in a potential suite of products to improve records management and data sharing in New York. In this vein, DCJS also realizes that the strategic long-term solution for fingerprint and mugshot submissions should utilize the electronic delivery system known as Store and Forward (S&F). A large portion of local agencies currently using SJS would benefit immediately and immensely by having an interface using this S&F technology. Images and data could then be transmitted both to DCJS and the FBI electronically with results usually returned within three hours. This not only provides greater safety for the officer and for the community, but also provides complete criminal history and wanted information for arraignment in a timely manner.

The goal of this document is to define an interface specification so that SJS can submit to Store and Forward. This capability is accomplished by utilization of an interface between SJS and an Integration Module (IM). The Integration Module (IM) is third party server software that can communicate with DCJS via an interface defined in the New York State Criminal Justice Electronic Fingerprint Transmission Standard (NYSCJEFTS). A copy of the NYSCJEFTS can be found at the DCJS website. The links are <http://www.criminaljustice.state.ny.us/advtech/efts.htm> or <http://www.criminaljustice.state.ny.us/advtech/efts.pdf>. NYSCJEFTS uses a tagging mechanism developed by NIST (National Institute for Standards and Technology). It is similar in nature to XML (eXtensible Markup Language) in that each field has a tag so the receiving application knows what fields are in the record. Using the NIST format, the Integration Module has the ability to convert data fields into a NYSCJEFTS record and transmit it to DCJS. The Integration Module also has the ability to receive and handle response messages sent by DCJS. The Integration Module is independent of the various components connected to the server, such as livescan, cardscan, and a mugshot system, and is not proprietary to any specific vendor.

The SJS system is the core data repository for any participating law enforcement agency. The Integration Module is intended as a complement to SJS by offering the capability to electronically submit to and process responses from DCJS. In order to best leverage the benefit to the law enforcement agency, it is imperative that SJS and the Integration Module pass data between them. With this exchange of data, double entry is eliminated. Not only does this make the operations of the contributor more efficient, it also ensures that accurate and timely data is disseminated to the arresting agency, court, and DA.

SJS Interface Specification

The SJS application is the initial entry point of data, and the Integration Module acts as a gateway to DCJS to transfer fingerprints and related information. In this case, SJS would be exporting the data and the Integration Module would be importing the initial information.

Once the Integration Module receives the processing response from DCJS, there should be a provision that would allow the Integration Module to pass the NYSID and FBI numbers, Identification result, and Criminal Justice Tracking number (arrests only) to SJS. The DCJS response will also be joined with the SJS arrest number kept by the Integration Module to help link back to the SJS system.

2. Business Flow

In order to be compatible, each system must be able to either import or export common data. Each system would write locally to their data storage and import from a remote data storage. This architecture allows one system to be down while the other is still functioning.

SJS is the primary data capture source and the IM is importing data from SJS. The operator (arresting agency employee) would enter all information into SJS. The operator would then select an option from the SJS menu to commence the livescan / cardscan export. At this point, the Integration Module would be responsible for importing the data into its records. The operator would use vendor supplied software to acquire the fingerprints (and as an auxiliary function, mugshots) and send the NYSCJEFTS submission to DCJS. DCJS will reply to the EFTS submission with an acknowledgement, a rejection, or an identification result (including non-idents) to the Integration Module. The Integration Module would then export the DCJS response data to the SJS application, allowing SJS to incorporate returned data into the SJS database. The SJS application will need to determine conflict resolution between SJS transmitted data and DCJS returned data. For example, SJS might submit a NYSID that is different from the NYSID returned in the DCJS response.

The SJS application generates an incident number and an arrest number for the arrested subject. These numbers will be used as a common link between the Integration Module and SJS.

The Integration Module System is not required to have persistent storage of the records.

3. Operating System

The SJS application is currently certified for Windows NT 4.0 and Windows 2000 Professional Server.

4. File-Based Transfers

Data will be transferred between systems through files. Both the SJS application and the Integration Module will have the ability to import data from the exporting system.

The advantage to having file-based transfers is the ability to continue work even when there is a communications failure between SJS and the Integration Module. A communications failure should not affect either system in any way. Since both systems will write all data to their local export directories, the updated records would remain until transferred to the other system. However, it is important to note that during a time when no communications link exists, neither system will be able to update the other system's records until the link is restored. Upon successful communication with the importing system, the record(s) would be transferred to the importing system which would then assimilate the data.

SJS Interface Specification

Transportation of records between the two systems will occur using either an SMB connection or Windows file sharing.

A. SMB Connectivity Information

The IM server's choice of operating system could be Unix/Linux. This presents a problem since SJS runs on a Windows-based operating system. If performing a file-based transfer using Network File System (NFS), the NT system must have a method by which to connect to the IM server for these transfers.

Where the IM's operating system is Unix/Linux, a SMB connection must be implemented to handle communication between the servers. SMB is used to provide network services to SMB (sometimes called "Lan Manager") clients, including various versions of MS Windows, OS/2, and other Linux machines (Figure 1). SMB uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need NetBEUI (Microsoft Raw NetBIOS frame) protocol.

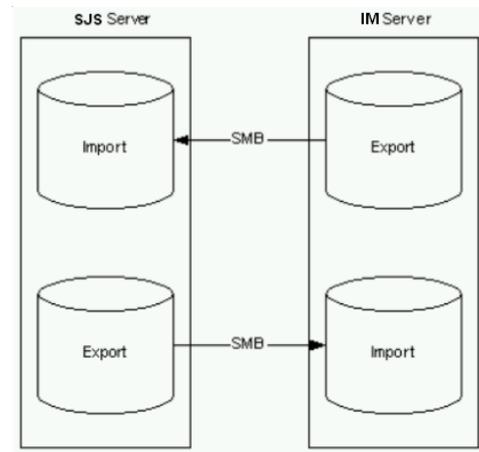


Figure 1 - SMB Transport

For more information on SMB, please visit <http://www.samba.org>.

B. Windows Server

If the Integration Module server is a Windows Server, then the normal Windows directory and file sharing will apply.

5. Directory Structure

The SJS application and the Integration Module will each need to create an export directory on their respective servers. Each system will need to give the other system access to the export directory.

For every arrest saved by the SJS application or identification result received by the Integration Module and forwarded to the SJS application, a directory will be created (in the export directory) based on a 14-digit sequence number. The 14-digits will consist of CCYYMMDDHHMMSS, where:

CC	–	2-digit century	(e.g. "20")
YY	–	2-digit year	(e.g. "02")
MM	–	2-digit month	(e.g. "03")
DD	–	2-digit day	(e.g. "04")
HH	–	2-digit hour	(e.g. "05")
MM	–	2-digit minute	(e.g. "06")
SS	–	2 digit second	(e.g. "07")

Upon creation of this directory, the file extension will be named ".LOCK". This is to ensure that the importing system does not begin transferring information from the directory while the creating system is writing files to the directory. Once SJS has completed the file exports, the system will rename this directory's extension to ".READY". Therefore, the creating system is responsible for writing contents to the directory while it is locked. The consuming system will be responsible for

SJS Interface Specification

directory contents once the directory is renamed to “.READY”. The consumer system is then responsible for removal of the directory upon completion of processing that directory’s contents. Since it may be possible for both an insert and multiple updates to exist at the same time, it is important that the Integration Module be able to read and process the directories in ascending order. This will ensure that the last record read for a given event is the most up-to-date. The same holds true for the SJS system. SJS must process the response from the Integration Module in ascending order.

The “.READY” directory will contain XML and JPG files. Demographic, Arrest, and Transaction data will be placed in a file named “record.xml”. This file will be formatted using the XML protocol. XML stands for **EX**tensible **M**arkup **L**anguage. XML is a markup language such as HTML, but its main purpose is to describe data and has become a standard for doing so. The file is in ASCII format.

The mugshot image file, which is optional, will have the extension “.JPG”. The “record.xml” file will reference the name of the image file. The image file will be located in the same directory as the “record.xml”. Release v1.2 will import mugshots into SJS. The file name must be mugshot.jpg and the size of the jpg cannot be more than 32K for versions of SJS 6.5 or less.

The exact structure of the file “record.xml” is described in Appendix A.

6. Transactions

The “record.xml” file will contain an attribute that describes what type of transaction is occurring. That attribute is called “InterfaceTransaction” and can have the following values:

6.1 SJS to Integration Module (IM)

- 6.1.1 ADD – The user added (created) an arrest record. Even when changes are made, SJS will create an ADD transaction type record. IMs with persistent storage will need to determine if a record for a particular arrest already exists. If a record exists then the ADD becomes an update rather than an insert. IMs without persistent storage will need to display the last ADD file sent so the user gets the most current data.
- 6.1.2 DELETE – The user deleted an arrest record in the SJS system. This is an auxiliary function and will be handled only if the Integration Module has persistent storage.
- 6.1.3 SEAL – The user sealed an arrest record in the SJS system. This is an auxiliary function and will be handled only if the Integration Module has persistent storage.

6.2 Integration Module (IM) to DCJS

The Integration Module is responsible for the NYSCJEFTS submissions to DCJS. The SJS system must define the Store and Forward ‘Type of Transaction’ (TOT). The “record.xml” file has an attribute named TOT, which correlates with the Store and Forward Type of Transaction (TOT). The following TOT’s will be handled:

- 6.2.1 CARAAR - Adult Arrest Submission
- 6.2.2 CARJDR - Juvenile Delinquent Submission
- 6.2.3 CARCIR - Criminal Inquiry¹
- 6.2.4 CARADM - Institution Admissions²
- 6.2.5 CARREL - Institution Release Submission²

SJS Interface Specification

6.2.6 FBICRM - FBI Arrest Resubmission³

¹ This is an auxiliary function awaiting additional development to SJS.

² Auxiliary function awaiting DCJS development specifications.

³ Currently under development at DCJS. Expected operational April 2002

6.3 DCJS to Integration Module (IM)

6.3.1 SREACK - Transaction Accepted (SREACK)

This message is returned to indicate that DCJS has taken responsibility for the transaction and it may be removed from the Sender's transmission queue and the next transaction may now be submitted.

6.3.2 SRENYS - New York State's Identification Processing Results

This message contains the results of DCJS' identification process, including identification or non-identification, NYSID, and the present status of the individual on Interstate Identification Index (III).

6.3.3 ERRREJ - Transaction Error (ERRREJ)

This transaction is returned by DCJS to indicate either that the submitted transaction cannot be accepted (usually data or formatting errors) or that a transaction error was detected during processing (usually due to unacceptable fingerprint images).

6.4 Integration Module (IM) to SJS

6.4.1 IDENT – DCJS returned an Identification message, which could be either an Identification or Non-Identification of a person, to the Integration Module. The Integration Module will provide the Identification result, CJTN, SJS Arrest Number, NYSID Number, and FBI Number (if available).

6.4.2 REJECT – There has been a rejection from DCJS for the submission. The IM will provide the CJTN, SJS Arrest Number, and Reject Reason.

6.4.3 ACK – There has been an acknowledgement from DCJS that it has received the submission. The Integration Module will provide the CJTN (optional – Arrests only) and the SJS Arrest Number.

6.4.4 Do not send back a response for Delete and Seal transactions types.

7. File Structure

The structure of the "record.xml" file is described in Appendix A. This appendix shows the XML structure of the file and lists all the attributes that are required. The individual fields and their relationship to the NYSCJEFTS are described in Appendix B. All data elements will conform to NYS Data Standards unless otherwise noted.

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

APPENDIX A

```

<?xml version="1.0" encoding="UTF-8" ?>
- <Record>
  //Transaction Information
  <InterfaceTransaction>.....</InterfaceTransaction>
  <Resubmission>.....</Resubmission>
  <SubmittingAgency>.....</SubmittingAgency>
  <SubmittingEmployeeID>...</SubmittingEmployeeID>
  <TOT>.....</TOT>
  <Contributor>.....</Contributor>
  //Response Errors
- <Errors>
  // Multiple Errors can be returned from DCJS
  - <Error>
    <ResponseErrorCode>....</ResponseErrorCode>
    <ResponseErrorDesc>....</ResponseErrorDesc>
  </Error>
</Errors>
  //Arrest Table Information
  <ArrestDate>.....</ArrestDate>
  <PhotographNumber>.....</PhotographNumber>
  <AgencyDivision>.....</AgencyDivision>
  <ArrestType>.....</ArrestType>
  <ArrestingAgency>.....</ArrestingAgency>
  <FOAAgencyORI>.....</FOAAgencyORI>
  <FOAAgencyName>....</FOAAgencyName>
  <DIR>....</DIR>
  <ArrestNumber>.....</ArrestNumber>
  <ArrestingOfficerID>...</ArrestingOfficerID>
  <AssistingOfficerID>...</AssistingOfficerID>
  <AssistingAgencyORI>...</AssistingAgencyORI>
  <CJTN>.....</CJTN>
  <ArrestStatus>....</ArrestStatus>
  <CourtOfArraignment>...</CourtOfArraignment>
  <CourtOfJurisdiction>..</CourtOfJurisdiction>
  <DateOfArraignment>.....</DateOfArraignment>
  //Arrest Weapons Information
- <ArrestWeapons>
  //You can have multiple "Weapon" Objects
  <Weapon>....</Weapon>
</ArrestWeapons>
  //Arrest Location Information
- <ArrestLocation>
  - <xsl:for-each select="ArrestLocation/ArrestLocation_ROW">
    - <StreetNumber>

```

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

```

    <xsl:value-of select="StreetNumber" />
  </StreetNumber>
- <StreetName>
  <xsl:value-of select="StreetName" />
  </StreetName>
- <Building>
  <xsl:value-of select="Building" />
  </Building>
- <Apartment>
  <xsl:value-of select="Apartment" />
  </Apartment>
- <City>
  <xsl:value-of select="City" />
  </City>
- <State>
  <xsl:value-of select="State" />
  </State>
- <Zip>
  <xsl:value-of select="Zip" />
  </Zip>
- <CTVCode>
  <xsl:value-of select="CTVCode" />
  </CTVCode>
</xsl:for-each>
</ArrestLocation>
//Person Master Information
- <PersonMaster>
  <FBINumber>.....</FBINumber>
  <SSN>.....</SSN>
  <DOB>.....</DOB>
  <NYSIDNumber>....</NYSIDNumber>
//Name Information
- <PersonName>
  <LastName>.....</LastName>
  <FirstName>.....</FirstName>
  <MiddleName>.....</MiddleName>
  <Suffix>.....</Suffix>
</PersonName>
//Person Detail
- <PersonDetail>
  <Height>.....</Height>
  <Weight>.....</Weight>
  <Sex>.....</Sex>
  <Build>.....</Build>
  <Race>.....</Race>
  <SkinTone>.....</SkinTone>
  <EthnicOrigin>.....</EthnicOrigin>

```

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

```

<Age>.....</Age>
<AgeRange>.....</AgeRange>
<BirthState>.....</BirthState>
<Citizenship>.....</Citizenship>
<EyeColor>.....</EyeColor>
<HairColor>.....</HairColor>
<MiscDesc>.....</MiscDesc>
<Scars>.....</Scars>
<Marks>.....</Marks>
<Tattoos>.....</Tattoos>
<CautionAndMedicalConditions>.....</CautionAndMedicalConditions>
<ConditionAtArrest>05</ConditionAtArrest>
<ResidentialStatus>U</ResidentialStatus>
<MaritalStatus>3</MaritalStatus>
<Education>1</Education>
<Occupation>LAB</Occupation>
<EmployedStatus>2</EmployedStatus>
<EmployerName>JOE EMPLOYER</EmployerName>
<EmployerStreetName>STREET1</EmployerStreetName>
<EmployerStreet2Name>STREET2</EmployerStreet2Name>
<EmployerBuildingName>BLD</EmployerBuildingName>
<EmployerApartmentName>123</EmployerApartmentName>
<EmployerCity>EMPLOYERVILLE</EmployerCity>
<EmployerState>NY</EmployerState>
<EmployerPostalCode>120651236</EmployerPostalCode>
<EmployerLocationCode>2350</EmployerLocationCode>
<EmployerTelephoneNumber>1236547897</EmployerTelephoneNumber>
<EmployerTelephoneSuffix>123</EmployerTelephoneSuffix>
<HomeTelephoneNumber>8457914143</HomeTelephoneNumber>
<BailAmount>200000</BailAmount>
<SearchWarrant>NO</SearchWarrant>
<Statement>WRITTEN</Statement>
<WarrantNumber>123654</WarrantNumber>
<Religion>300</Religion>
//Address Information
= <HomeAddress>
  <StreetNumber>...</StreetNumber>
  <StreetName>.....</StreetName>
  <Building>.....</Building>
  <Apartment>.....</Apartment>
  <City>.....</City>
  <State>.....</State>
  <County>.....</County>
  <Country>.....</Country>
  <ZipCode>.....</ZipCode>
  <CTVCode> .....</CTVCode>

```

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

```

    </HomeAddress>
  </PersonDetail>
  = <Alias>
    //You can have multiple "Name" Objects
    = <AliasName>
      <LastName>.....</LastName>
      <FirstName>.....</FirstName>
      <MiddleName>.....</MiddleName>
      <Suffix>.....</Suffix>
    </AliasName>
  </Alias>
</PersonMaster>
//Warrant Information
= <Warrants>
  //You can have multiple "Warrant" Objects
  = <Warrant>
    <WarrantDate>....</WarrantDate>
    <WarrantNumber>..</WarrantNumber>
    <WarrantORI>.....</WarrantORI>
  </Warrant>
</Warrants>
//Incident Information
= <Incidents>
  //You can have multiple "Incident" objects
  = <Incident>
    <IncidentNumber>.....</IncidentNumber>
    <OccurrenceDateStart>...</OccurrenceDateStart>
    <ArresteeNumber>.....</ArresteeNumber>
  //Address Information
  = <CrimeLocation>
    = <xsl:for-each
      select="CrimeLocation/CrimeLocation_ITEM">
      = <StreetNumber>
        <xsl:value-of select="StreetNumber" />
      </StreetNumber>
      = <StreetName>
        <xsl:value-of select="StreetName" />
      </StreetName>
      = <Building>
        <xsl:value-of select="Building" />
      </Building>
      = <Apartment>
        <xsl:value-of select="Apartment" />
      </Apartment>
      = <City>
        <xsl:value-of select="City" />
    </xsl:for-each>
  </CrimeLocation>
  </Incident>
</Incidents>

```

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

```

    </City>
  = <State>
    <xsl:value-of select="State" />
  </State>
  = <Zip>
    <xsl:value-of select="Zip" />
  </Zip>
  = <CTVCode>
    <xsl:value-of select="CTVCode" />
  </CTVCode>
</xsl:for-each>
</CrimeLocation>
//Arrest Charges Information
  = <Charges>
    //Arrest Charges can have multiple objects
    = <Charge>
      <Counts>.....</Counts>
      <Law>.....</Law>
      <Section>.....</Section>
      <SubSection>.....</SubSection>
      <Attempt>.....</Attempt>
      <Class>.....</Class>
      <Category>.....</Category>
      <Degree>.....</Degree>
      <NCICCode>.....</NCICCode>
      <Fingerprintable>.....</Fingerprintable>
    </Charge>
  </Charges>
</Incident>
</Incidents>

//Mugshot Information
  = <Mugshots>
    //You can have multiple Mugshot Objects
    = <Mugshot>
      <Type>.....</Type>
      <ImageFlag>.....</ImageFlag>
      <PrimaryImageFlag>..</PrimaryImageFlag>
      <ImageFilename>.....</ImageFilename>
    </Mugshot>
  </Mugshots>

// NYS Identification Results
  = <IdentificationResult>
    <IdentNYSID>....</IdentNYSID>
    <IdentFBINumber>...</IdentFBINumber>
    <IdentSearchResults>...</IdentSearchResults>

```

SJS Interface Specification

Appendix A

XML layout for "Record.XML"

```
</IdentificationResult>  
</Record>
```

SJS Interface Specification**Appendix B****SJS Data mapping to NYSCJEFTS****APPENDIX B**

XML Tag	EFTS Tag No.	CARAAR & FBICRM Mandatory / Optional	CARJDR Mandatory / Optional	CARCIR Mandatory / Optional	Comment(s)
Record					
Transaction Information					
InterfaceTransaction		M	M	M	This field is mandatory for the interface (see specification for details)
Resubmission	2.1000	3	3	3	Y/N value
TCN					
SubmittingAgency	1.08	M	M	M	
SubmittingEmployeeID	2.1004	M	M	M	
TOT	1.04	M	M	M	See section 6.2 of this specification
Contributor	2.1199	M	M	M	
Errors					
ResponseErrorCode	2.1090				See NYSCJEFTS for values
ResponseErrorDesc	2.60				See NYSCJEFTS for values
ArrestDate	2.0045	M	M		
Arrest Information					
ArrestDate	2.0045	M	M	O	
PhotographNumber	2.1077	O	O	O	
AgencyDivision	2.1203	O	O	O	
ArrestType	2.1209	2	2		Coded Value – See Data Dictionary
ArrestingAgency	2.1201	M	M		
FOAAgencyORI					
FOAAgencyName					
DIR	2.1226	2	2		Y/N
ArrestNumber	2.1210	O	O		
ArrestingOfficerID	2.1204	M	M		
AssistingOfficerID					Assisting Officer Id not used for Livescan/Cardscan
AssistingAgencyORI	2.1222	O	O		Agency assisting in arrest is not currently captured in SJS.
CJTN	2.1217	2	2		
ArrestStatus					Coded Value – See Data Dictionary
CourtOfArrest	2.1216	M			
CourtOfJurisdiction	2.1218	4	4		
DateofArrest **	2.1225	2	2		
Arrest Weapons					
Weapon	2.1211	O	O		Coded Value – See Data Dictionary

SJS Interface Specification**Appendix B****SJS Data mapping to NYSCJEFTS**

XML Tag	EFTS	CARAAR & FBICRM	CARJDR	CARCIR	
	Tag No.	Mandatory / Optional	Mandatory / Optional	Mandatory / Optional	Comment(s)
ArrestLocation					
StreetNumber					
StreetName					
Building					
Apartment					
City					
State					
Zip					
CTVCode	2.1206	M			Coded Value – See Data Dictionary
PersonMaster					
FBINumber	2.0014	O	O	O	
SSN	2.0016	2	2	2	
DOB **	2.0022	M	M	M	
NYSIDNumber	2.1101	2	2	2	
PersonName					
LastName	2.1110 (A)	M	M	M	
FirstName	2.1110 (B)	M	M	M	
MiddleName	2.1110 (C)	M	M	M	
Suffix	2.1110 (E)	M	M	M	Coded Value – See Data Dictionary
PersonDetail					
Height	2.0027	2	2	2	
Weight	2.0029	2	2	2	
Sex	2.1112	M	M	M	Coded Value – See Data Dictionary
Build					Coded Value – See Data Dictionary
Race	2.1113	M	M	M	Coded Value – See Data Dictionary
SkinTone	2.1114	2	2	2	Coded Value – See Data Dictionary
EthnicOrigin	2.1115	2	2	2	Coded Value – See Data Dictionary
Age	2.1116	5	5	5	
AgeRange	2.23	5	5	5	
BirthState	2.1117	2	2	2	Coded Value – See Data Dictionary
Citizenship	2.1118	O	O		Coded Value – See Data Dictionary
EyeColor	2.1120	2	2	2	Coded Value – See Data Dictionary
HairColor	2.1121	O	O	2	Coded Value – See Data Dictionary
MiscDesc	2.1123 (A,B,C,D)	O	O	O	
Scars	2.1126	O	O	O	
Marks	2.1126	O	O	O	
Tattoos	2.1126	O	O	O	

SJS Interface Specification

Appendix B

SJS Data mapping to NYSCJEFTS

XML Tag	EFTS Tag No.	CARAAR & FBICRM Mandatory / Optional	CARJDR Mandatory / Optional	CARCIR Mandatory / Optional	Comment(s)
CautionAndMedicalConditions	2.1149	O	O		Coded Value – See Data Dictionary
ConditionAtArrest					Coded Value – See Data Dictionary Defendants Physical Condition
ResidentialStatus					Coded Value – See Data Dictionary ARRESTEE RESIDENCE STATUS
Marital Status					Coded Value – See Data Dictionary
Education					See Appendix D
Occupation					See Appendix D
EmployedStatus					Coded Value – See Data Dictionary
EmployerName					
EmployerStreetName					
EmployerStreetName2					
EmployerBuildingName					
EmployerApartmentName					
EmployerCity					
EmployerState					
EmployerPostalCode					
EmployerLocationCode					
EmployerTelephoneNumber					
HomeTelephoneNumber					
BailAmount					
SearchWarrant					See Appendix D
Statement					See Appendix D
Warrant Number					
Religion					Coded Value – See Data Dictionary
HomeAddress					
StreetNumber	2.1130(A)	2	2	2	
StreetName	2.1130(A)	2	2	2	
Building	2.1130(B)	2	2	2	
Apartment	2.1130(B)	2	2	2	
City	2.1130(C)	2	2	2	
State	2.1130(E)	2	2	2	Coded Value – See Data Dictionary
County	2.1130(D)	2	2	2	Coded Value – See Data Dictionary
Country	2.1130(E)	2	2	2	Coded Value – See Data Dictionary
ZipCode	2.1130(F)	2	2	2	
CTVCode					No matching EFTS
AliasName					
LastName	2.1111(A)	O	O	O	
FirstName	2.1111(B)	O	O	O	
MiddleName	2.1111(C)	O	O	O	
Suffix	2.1111(E)	O	O	O	See NYSCJEFTS – Table T9

SJS Interface Specification**Appendix B****SJS Data mapping to NYSCJEFTS**

XML Tag	EFTS Tag No.	CARAAR & FBICRM Mandatory / Optional	CARJDR Mandatory / Optional	CARCIR Mandatory / Optional	Comment(s)
Warrant					
WarrantDate **	2.1215(B)	O	O		
WarrantNumber	2.1215(C)	O	O		
WarrantORI	2.1215(A)	O	O		
Incident					
IncidentNumber	2.1223(A)	M	M		
OccurrenceDateStart **	2.1223(B)	M	M		
ArresteeNumber	2.1223(D)	M	M		
CrimeLocation					
StreetNumber					
StreetName					
Building					
Apartment					
City					
State					
Zip					
CTVCode	2.1223(C)	M	M		Coded Value – See Data Dictionary
Charge					
					Coded Value from Coded Law Tables
Counts	2.1223(M)	M	M		
Law	2.1223(E)	M	M		
Section	2.1223(F)	M	M		
SubSection	2.1223(G)	M	M		
Attempt	2.1223(K)	M	M		
Class	2.1223(H)	M	M		
Category	2.1223(I)	M	M		
Degree	2.1223(J)	M	M		
NCICCode	2.1223(L)	M	M		
Fingerprintable					Y/N At least one charge has to be fingerprintable for the two arrest TOTs
Mugshots					
Type	10.3				See NYSCJEFTS for values
ImageFlag					Y/N
PrimaryImageFlag					Y/N - default to Y since SJS handles only 1 image
ImageFileName					
NYS Identification Results					
IdentNYSID	2.1101	6	6	6	

SJS Interface Specification

Appendix B

SJS Data mapping to NYSCJEFTS

XML Tag	EFTS	CARAAR & FBICRM	CARJDR	CARCIR	
	Tag No.	Mandatory / Optional	Mandatory / Optional	Mandatory / Optional	Comment(s)
IdentFBINumber	2.14	7	7	7	
IdentSearchResults	2.1100				Y/N

**** DATE FORMATS**

All dates will use the following format MM/DD/YYYY HH:MM:SS. For example, 2/2/1975 0:0:0 or 12/30/1999 8:46:0.

SJS Interface Specification

Appendix C

Appendix B Notes

APPENDIX C

Note Number	Description
1	This field may be included when fingerprint images are included in the transmission
2	This information should be included whenever known.
3	Only include this field when the transaction is a resubmission for a previously rejected transaction
4	Include only if different from Court of Arraignment (2.1216)
5	A value of "99" is interpreted as older than 98
6	Certain types of transactions do not always result in NYSID number. For example, a Criminal Inquiry that is not identified will not have a NYSID Number assigned.
7	If FBI response is not available at conclusion of DCJS processing, and the transaction was sent electronically to the FBI, a separate message may be sent via DCJS Secure Services when the FBI responds to DCJS.
M	Mandatory
O	Optional

SJS Interface Specification

Appendix D

SJS data mapping

APPENDIX D

Education

Description	Code
NONE OR KINDERGARTEN	0
GRADE SCHOOL (ENTER 01-08)	1
HIGH SCHOOL (ENTER 09 - 12)	9
COLLEGE YEARS (ENTER 13-16)	13
MORE THAN COLLEGE (MS, DR, ETC)	17
MORE THAN COLLEGE (MS, DR, ETC)	99

Occupation

	169
ENGINEERS, SURVEYORS AND ARCHITECTS	9
	179
NATURAL SCIENTIST AND MATHEMATICIANS	9
	199
SOCIAL SCIENTISTS/WORKERS RELIGIOUS WORKERS AND LAWYERS	9
	229
TEACHERS, LIBRARIANS AND COUNSELORS	9
	269
HEALTH DIAGNOSING AND TREATING PRACTITIONERS	9
REGISTERED NURSES PHARMACISTS DIETITIANS THERAPISTS AND PHYSICIANS	299
ASSISTS	9
	329
WRITERS	9
	369
HEALTH TECHNOLOGISTS AND TECHNICIANS	9
	379
TECHNOLOGISTS AND TECHNICIANS EXCEPT HEALTH	9
	409
MARKETING AND SALES OCCUPATIONS	9
	459
ADMINISTRATIVE SUPPORT OCCUPATIONS INCLUDING CLERICAL	9
	509
SERVICE OCCUPATIONS	9
	559
AGRICULTURE FORESTRY AND FISHING OCCUPATIONS	9
	609
MECHANICS AND REPAIRERS	9
	639
CONSTRUCTION AND EXTRACTIVE OCCUPATIONS	9
	679
PRECISION PRODUCTION OCCUPATIONS	9
	719
PRODUCTION WORKING ARTISTS OCCUPATIONS ENTERTAINERS AND ATHLETES	9
	819
TRANSPORTATION AND MATERIAL MOVING OCCUPATIONS	9

SJS Interface Specification

Appendix D SJS data mapping

HANDLERS EQUIPMENT CLEANERS HELPERS AND LABORERS	859
	9
MILITARY OCCUPATIONS	910
CLERICAL	0
CRAFTSMAN	CLK
LABORER	CRA
EXECUTIVE, ADMIN AND MANAGERIAL OCCUPATIONS	LAB
MISCELLANEOUS OCCUPATIONS	MAN
OPERATIVE	MSC
PROFESSIONAL	OPR
STUDENT	PRO
UNKNOWN	STU
NOT REPORTED	U
	XXX

Search Warrant

Yes
No
Unknown

Statement

Verbal
Written
Both
None

This page reserved for ACISS Data Structure information

Proposed Staffing and Title Thresholds

Bidders should use the descriptions in this document for completion of the **Staffing Plan**, and as a guideline for completing the **Hourly Rates for Additional Phases/Task Orders** component of the Cost Proposal.

For each job described below at least ½ of the noted experience must be with the Bidder’s RMS application:

Project Manager – Minimum of 4 years experience in overseeing large scaled projects comprised of sub-projects and distinct deliverables; typically coordinates and delegates the assignments for the project staff numbering over 10; focal point of contact for Issuing Entity regarding project status, meetings, reporting requirements; scope changes, and financial, administrative, and technical issues and concerns raised by project staff or Issuing Entity.

Technical Architect - Minimum of 4 years experience with designing, building and problem resolving in large scale application infrastructures; environments include but are not limited to mainframe, server, web, personal computers, laptops, and mobility devices.

Database Administrator - Minimum of 4 years experience in database administration.

Programmer - Minimum of 4 years experience with writing application software, data analysis, data access, data structures, data manipulation, databases, design, programming, testing and implementation, technical and user documentation, software conversions; environments include but are not limited to mainframe, server, web, personal computers, laptops, and mobility devices.

Business Analyst - Minimum of 4 years experience with assisting and/or leading in the design of program specifications and business process review; able to assist with application testing, technical and user documentation, software conversions; environments include but are not limited to mainframe, mid range, personal computers, laptops.

Trainer - Minimum of 2 years experience in application and business process training.

Tester - Minimum of 2 years experience in unit, integrated, system and acceptance testing.

Technical Writer - Minimum of 2 years experience with writing technical and user documentation.

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Adams Vg PD	0	5	5			X	5
Addison Vg PD	3	5	8			X	8
Afton Vg PD					X		
Akron Vg PD	1	13	14			X	14
Albany City PD	322	0	322			X	322
Albany County Sheriff	118	0	118	118	X		
Albion Vg PD					X		
Alexandria Bay Vg PD	2	11	13	13	X		
Alfred Vg PD	6	8	14	14	X		
Alleghany County Sheriff	26	0	26	26	X		
Alleghany Vg PD	2	10	12	12	X		
Altamont Vg PD	1	11	12	12	X		
Amherst Town PD	153	0	153			X	153
Amityville Vg PD	23	1	24			X	24
Amsterdam City PD	39	0	39			X	39
Andover Vg PD					X		
Angelica Vg PD						X	
Arcade Vg PD	6	4	10			X	10
Ardsley Vg PD	19	0	19			X	19
Asharoken Vg PD	3	8	11			X	11
Ashokan PCT (NYC-BWSP)	193	0	193			X	193
Athens Vg PD					X		
Attica Vg PD	5	6	11	11	X		
Auburn City PD	62	0	62			X	62
Avon Vg PD					X		
Bainbridge Vg PD					X		
Baldwinsville Vg PD	10	0	10			X	10
Ballston Spa Vg PD	5	11	16	16	X		
Barker Village Police Department						X	
Batavia City PD	28	0	28			X	28
Bath Vg PD	10	6	16			X	16
Beacon City PD	31	0	31			X	31
Bedford Town PD	38	0	38			X	38
Belmont Vg PD					X		
Bethlehem Town PD	37	0	37			X	37
Binghamton City PD	122	0	122			X	122
Black River Village Police Department						X	
Blooming Grove Town PD	14	0	14			X	14
Bolivar Vg PD	1	7	8	8	X		
Bolton Town PD	0	4	4			X	4

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Boonville Vg PD	3	3	6			X	6
Brant Town PD	1	16	17			X	17
Brewster Vg PD	0	15	15	15	X		
Briarcliff Manor Vg PD	19	0	19			X	19
Brighton Town PD	40	0	40			X	40
Brockport Vg PD	11	2	13			X	13
Bronxville Vg PD	21	0	21			X	21
Broome County Sheriff	53	0	53			X	53
Brownville Village Police Department						X	
Buchanan Vg PD					X		
Buffalo City PD	759	0	759			X	759
Cairo Town PD	1	12	13	13	X		
Caledonia Vg PD	3	3	6	6	X		
Cambridge Vg PD	6	11	17	17	X		
Camden Vg PD	3	9	12	12	X		
Camillus Town and Vg PD	23	6	29			X	29
Canajoharie Vg PD	3	12	15	15	X		
Canandaigua City PD	23	2	25	25	X		
Canastota Vg PD	5	10	15	15	X		
Canisteo Vg PD	2	2	4			X	4
Canton Vg PD					X		
Cape Vincent Vg PD						X	
Carmel Town PD	35	0	35			X	35
Carroll Town PD	0	5	5			X	5
Carthage Vg PD	4	5	9	9	X		
Caton Town Constabulary						X	
Catskill Vg PD	15	2	17	17	X		
Cattaraugus County Sheriff	68	39	107			X	107
Cattaraugus Vg PD	0	6	6			X	6
Cayuga County Sheriff	39	0	39			X	39
Cayuga Heights Vg PD						X	
Cazenovia Vg PD	4	12	16	16	X		
Central Square Vg PD	0	11	11	11	X		
Centre Island Vg PD	7	1	8			X	8
Chatham Vg PD	1	24	25	25	X		
Chautauqua County Sheriff	57	6	63			X	63
Cheektowaga Town PD	128	0	128			X	128
Chemung County Sheriff	45	0	45			X	45
Chenango County Sheriff	24	3	27			X	27
Chester Town PD	13	5	18			X	18

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Chester Vg PD						X	
Chittenango Vg PD	3	20	23	23	X		
Cicero Town PD						X	
Clarkstown Town PD	159	0	159			X	159
Clayton Vg PD	3	2	5	5	X		
Clifton Springs Vg PD	2	3	5	5	X		
Clinton County Sheriff					X		
Clyde Vg PD	0	8	8	8	X		
Cobleskill Vg PD	11	0	11	11	X		
Coeymans Town PD	4	18	22	22	X		
Cohocton Town Police Department						X	
Cohoes City PD					X		
Colchester Town PD	2	0	2			X	2
Cold Spring Vg PD	0	13	13	13	X		
Colonie Town PD	106	0	106			X	106
Columbia County Sheriff					X		
Cooperstown Vg PD					X		
Corfu Village Police Department						X	
Cornell University Police	46	0	46			X	46
Corning City PD	21	0	21			X	21
Cornwall Town PD	10	9	19			X	19
Cornwall-On-Hudson Vg PD						X	
Cortland City PD	42	0	42			X	42
Cortland County Sheriff	33	8	41			X	41
Coxsackie Vg PD	0	17	17	17	X		
Crawford Town PD	8	11	19			X	19
Croton On Hudson Vg PD	20	0	20			X	20
Cuba Town PD	4	11	15	15	X		
Dansville Vg PD	5	2	7	7	X		
Deer Park Town PD	4	17	21			X	21
Delaware County Sheriff	16	11	27	27	X		
Delhi Vg PD	4	10	14	14	X		
Depew Vg PD	29	0	29			X	29
Deposit Vg PD	1	7	8	8	X		
Dewitt Town PD	36	0	36			X	36
Dexter Vg PD						X	
Dobbs Ferry Vg PD	24	0	24			X	24
Dolgeville Vg PD	2	18	20	20	X		
Dryden Vg PD	6	8	14			X	14
Dunkirk City PD	37	0	37			X	37

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Durham Town PD	0	10	10	10	X		
Dutchess County Sheriff	95	43	138			X	138
East Aurora-Town Of Aurora PD	15	1	16			X	16
East Fishkill Town PD	32	0	32			X	32
East Greenbush Town PD	24	0	24			X	24
East Hampton Town PD	63	4	67			X	67
East Hampton Vg PD	23	0	23			X	23
East Rochester Vg PD	9	6	15			X	15
East Syracuse Vg PD	6	8	14			X	14
Eastchester Town PD	45	0	45			X	45
Eden Town PD	4	10	14			X	14
Ellenville Vg PD	10	14	24			X	24
Ellicott Town PD	12	10	22			X	22
Ellicottville Town PD	3	12	15	15	X		
Elmira City PD	79	0	79			X	79
Elmira Heights Vg PD	9	0	9			X	9
Elmira Town PD	4	3	7			X	7
Elmsford Vg PD	18	0	18	18	X		
Endicott Vg PD	35	0	35			X	35
Erie County Medical Center Police Department						X	
Erie County Sheriff	140	10	150			X	150
Essex County Sheriff	21	0	21	21	X		
Evans Town PD	24	5	29			X	29
Fairport Vg PD	10	0	10			X	10
Fallsburgh Town PD	20	0	20	20	X		
Fishkill Town PD	0	45	45			X	45
Fishkill Vg PD	0	25	25	25	X		
Floral Park Vg PD	34	0	34			X	34
Florida Vg PD	1	12	13			X	13
Fort Edward Vg PD	5	7	12	12	X		
Fort Plain Vg PD	4	12	16	16	X		
Frankfort Town PD					X		
Frankfort Vg PD	4	10	14	14	X		
Franklin County Sheriff	43	10	53	53	X		
Franklinville Vg PD	2	9	11	11	X		
Fredonia Vg PD	14	5	19			X	19
Freeport Vg PD	86	0	86			X	86
Friendship Town PD	0	8	8	8	X		
Fulton City PD	33	0	33			X	33
Fulton County Sheriff	24	9	33	33		X	

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Galway Village Police Department					X		
Garden City Vg PD	50	0	50			X	50
Gates Town PD	29	0	29			X	29
Geddes Town PD	14	2	16			X	16
Genesee County Sheriff	48	0	48			X	48
Geneseo Vg PD	7	4	11			X	11
Geneva City PD	36	0	36			X	36
Germantown Town PD	0	5	5	5	X		
Glen Cove City PD	50	0	50			X	50
Glen Park Vg PD	0	1	1			X	1
Glens Falls City PD	31	0	31			X	31
Glenville Town PD	22	0	22	22	X		
Gloversville City PD	29	0	29			X	29
Goshen Town PD						X	
Goshen Vg PD	16	4	20			X	20
Gouverneur Vg PD					X		
Gowanda Vg PD	0	18	18	18	X		
Grand Island Town Police Department						X	
Granville Vg PD	5	5	10	10	X		
Great Neck Estates Vg PD	12	0	12			X	12
Greece Town PD	98	0	98			X	98
Green Island Vg PD	0	23	23	23	X		
Greenburgh Town PD	113	0	113			X	113
Greene County Sheriff					X		
Greene Vg PD	1	3	4			X	4
Greenport Town PD					X		
Greenwich Vg PD	6	14	20	20	X		
Greenwood Lake Vg PD	7	9	16			X	16
Groton Vg PD	1	13	14			X	14
Guilderland Town PD	35	0	35			X	35
Hamburg Town PD	60	0	60			X	60
Hamburg Vg PD	13	0	13			X	13
Hamilton County Sheriff	5	2	7			X	7
Hamilton Vg PD	5	7	12	12	X		
Hammondsport Vg PD	0	2	2			X	2
Hancock Vg PD	0	4	4			X	4
Harriman Vg PD	7	3	10			X	10
Harrison Town PD	60	0	60			X	60
Hastings On Hudson Vg PD	20	0	20			X	20
Haverstraw Town PD	68	0	68			X	68

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Head Of Harbor Vg PD					X		
Hempstead Vg PD	119	0	119			X	119
Herkimer County Sheriff	5	5	10	10	X		
Herkimer Vg PD	21	7	28			X	28
Highland Falls Vg PD	9	11	20			X	20
Highlands Town PD	0	22	22			X	22
Holley Vg PD					X		
Homer Vg PD	4	7	11	11	X		
Hoosick Falls Vg PD	2	13	15	15	X		
Hornell City PD	22	0	22			X	22
Horseheads Vg PD	13	0	13			X	13
Hudson City PD	26	0	26			X	26
Hudson Falls Vg PD	13	4	17	17	X		
Hunter Town PD	2	10	12	12	X		
Huntington Bay Vg PD	4	9	13			X	13
Hyde Park Town PD						X	
Ilion Vg PD	18	0	18	18	X		
Independence Town PD	0	1	1	1	X		
Inlet Town PD	2	5	7	7	X		
Interlaken Vg PD	1	1	2			X	2
Irondequoit Town PD						X	
Irvington Vg PD	22	0	22			X	22
Ithaca City PD	65	0	65			X	65
Ithaca College PD	20	0	20			X	20
Jamestown City PD	60	0	60			X	60
Jefferson County Sheriff	44	0	44			X	44
Johnson City Vg PD	31	3	34			X	34
Johnstown City PD	24	0	24			X	24
Jordan Vg PD	0	7	7			X	7
Kenmore Vg PD	25	0	25			X	25
Kensington Vg PD	6	0	6			X	6
Kent Town PD	20	0	20			X	20
Kings Point Vg PD	22	0	22			X	22
Kingston City PD	73	0	73			X	73
Kirkland Town PD	7	9	16	16	X		
Lackawanna City PD	47	0	47			X	47
Lake Placid Vg PD	11	4	15			X	15
Lake Success Vg PD	21	0	21			X	21
Lakewood-Busti PD	9	10	19			X	19
Lancaster Town PD	50	0	50			X	50

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Larchmont Vg PD					X		
Le Roy Vg PD	7	5	12			X	12
Lewis County Sheriff	18	2	20	20	X		
Lewisboro Town PD	3	13	16	16	X		
Lewiston Town PD	9	8	17	17	X		
Liberty Vg PD	15	0	15	15	X		
Little Falls City PD	12	10	22			X	22
Liverpool Vg PD	4	10	14			X	14
Livingston County Sheriff	47	24	71			X	71
Lloyd Harbor Vg PD	12	0	12			X	12
Lloyd Town PD	8	14	22			X	22
Lockport City PD	51	0	51			X	51
Long Beach City PD						X	
Lowville Vg PD	6	8	14	14	X		
Lynbrook Vg PD	46	0	46			X	46
Lyons Vg PD	6	6	12	12	X		
Macedon Town and Vg PD	4	4	8	8	X		
Madison County Sheriff	32	43	75	75	X		
Malone Vg PD	14	0	14	14	X		
Malverne Vg PD	23	0	23			X	23
Mamaroneck Town PD	37	0	37			X	37
Mamaroneck Vg PD	49	7	56			X	56
Manchester Vg PD	0	1	1			X	1
Manlius Town PD						X	
Marcellus Vg PD	0	13	13			X	13
Marlborough Town PD	6	24	30	30	X		
Massena Vg PD	20	1	21	21	X		
Maybrook Vg PD	3	10	13	13	X		
McGraw Village Police Department						X	
Mechanicville City PD	12	9	21	21	X		
Medina Vg PD	11	1	12	12	X		
Menands Vg PD	11	4	15	15	X		
Metropolitan Transit Authority	666	0	666			X	666
Middleport Vg PD	3	3	6	6	X		
Middletown City PD	69	0	69			X	69
Millbrook Vg PD					X		
Millerton Village Police Department					X		
Mohawk Vg PD	4	13	17	17	X		
Monroe County Sheriff	272	57	329			X	329
Monroe Vg PD	17	0	17			X	17

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Montgomery County Sheriff	76	23	99			X	99
Montgomery Town PD	13	22	35			X	35
Montgomery Vg PD	0	28	28			X	28
Monticello Vg PD						X	
Moravia Vg PD	0	10	10	10	X		
Moriah Town PD	2	0	2			X	2
Mount Hope Town PD	4	13	17			X	17
Mount Kisco Vg PD	31	0	31			X	31
Mount Morris Vg PD	5	12	17	17	X		
Mount Pleasant Town PD	42	0	42			X	42
Mount Vernon City PD	207	0	207			X	207
Nassau County PD	2,247	0	2,247			X	2,247
Nassau County Sheriff's Office						X	
Nassau Vg PD	0	7	7	7	X		
New Berlin Town PD	0	9	9	9	X		
New Castle Town PD	36	0	36			X	36
New Hartford Town and Vg PD	19	7	26			X	26
New Paltz Town and Vg PD	19	8	27			X	27
New Rochelle City PD	158	0	158			X	158
New Windsor Town PD	40	0	40			X	40
New York City DEP Police					X		
New York City Police Department	34,555	0	34,555			X	34,555
New York Mills Vg PD	3	10	13	13	X		
New York State Regional Park Police	209	0	209		X		209
New York-New Jersey Port Authority						X	
Newark Vg PD	17	0	17	17	X		
Newburgh City PD	73	0	73			X	73
Newburgh Town PD	46	0	46			X	46
Niagara County Sheriff	106	1	107			X	107
Niagara Falls City PD	152	0	152			X	152
Niagara Town PD	4	21	25	25	X		
Niskayuna Town PD	27	0	27	27	X		
Nissequogue Vg PD						X	
Norfolk Town PD	0	10	10	10	X		
North Castle Town PD						X	
North Greenbush Town PD	16	1	17	17	X		
North Salem Town Police Department						X	
North Syracuse Vg PD	10	6	16			X	16
North Tonawanda City PD	45	0	45			X	45
Northeast T and Millerton V PD						X	

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Northport Vg PD	15	5	20			X	20
Northville Vg PD	0	10	10			X	10
Norwich City PD	19	0	19			X	19
Norwood Vg PD	0	9	9	9	X		
Nunda Town and Vg PD	0	12	12	12	X		
Ocean Beach Vg PD					X		
Ogden Town PD	12	1	13			X	13
Ogdensburg City PD	26	0	26	26		X	
Old Brookville Vg PD	26	0	26			X	26
Old Westbury Vg PD	26	0	26			X	26
Olean City PD						X	
Olive Town PD	1	9	10			X	10
Oneida City PD	23	0	23	23	X		
Oneida County Sheriff	81	2	83			X	83
Oneonta City PD	26	0	26			X	26
Onondaga County Park Rangers						X	
Onondaga County Sheriff						X	
Ontario County Sheriff	64	28	92			X	92
Orange County Sheriff	98	57	155			X	155
Orangetown Town PD	81	0	81			X	81
Orchard Park Town PD	29	0	29			X	29
Oriskany Vg PD	0	9	9	9	X		
Orleans County Sheriff					X		
Ossining Town Police Department						X	
Ossining Vg PD	55	0	55			X	55
Oswego City PD	41	0	41	41	X		
Oswego County Sheriff	66	24	90	90	X		
Otsego County Sheriff	16	1	17	17	X		
Owego Vg PD	8	9	17	17	X		
Oxford Vg PD	1	5	6			X	6
Oyster Bay Cove Vg PD	12	0	12			X	12
Painted Post Vg PD	3	5	8	8	X		
Palmyra Vg PD	5	0	5	5	X		
Peekskill City PD	57	0	57			X	57
Pelham Manor Vg PD	27	0	27	27	X		
Pelham Vg PD	25	0	25	25	X		
Penn Yan Vg PD	12	2	14			X	14
Perry Vg PD	4	11	15	15	X		
Phelps Vg PD						X	
Philmont Vg PD						X	

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Phoenix Vg PD						X	
Piermont Vg PD	8	2	10	10	X		
Pine Plains Town PD	0	9	9	9	X		
Plattekill Town PD	0	21	21			X	21
Plattsburgh City PD	48	0	48			X	48
Pleasantville Vg PD	21	0	21			X	21
Port Byron Vg PD	0	7	7	7	X		
Port Chester Vg PD	58	0	58			X	58
Port Dickinson Vg PD	4	6	10			X	10
Port Jervis City PD	30	0	30			X	30
Port Washington Police District	61	0	61			X	61
Portville Vg PD	0	7	7			X	7
Potsdam Vg PD	14	0	14	14	X		
Poughkeepsie City PD	100	0	100			X	100
Poughkeepsie Town PD	81	0	81	81	X		
Pound Ridge Town PD						X	
Pulaski Vg PD	1	9	10	10	X		
Putnam County Sheriff	83	4	87			X	87
Quogue Vg PD	13	6	19			X	19
Ramapo Town PD	106	0	106			X	106
Red Hook Vg PD	2	11	13			X	13
Rensselaer City PD	27	0	27			X	27
Rensselaer County Sheriff	33	0	33			X	33
Rensselaer Poly Tech Police	30	3	33			X	33
Rhinebeck Vg PD	0	12	12			X	12
Riverhead Town PD	85	12	97			X	97
Rochester City PD	741	0	741			X	741
Rockland County Sheriff	77	57	134			X	134
Rockville Centre Vg PD	51	0	51			X	51
Rome City PD	76	10	86			X	86
Rosendale Town PD	2	11	13			X	13
Rotterdam Town PD	41	0	41			X	41
Rouses Point Vg PD	1	0	1	1	X		
Rushford Town Police Department						X	
Rye Brook Vg PD	27	0	27			X	27
Rye City PD	34	0	34			X	34
Sackets Harbor Vg PD	0	8	8	8	X		
Sag Harbor Vg PD	13	3	16			X	16
Salamanca City PD	16	4	20	20	X		
Sands Point Vg PD	20	0	20			X	20

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Saranac Lake Vg PD	12	0	12	12	X		
Saratoga County Sheriff	112	0	112			X	112
Saratoga Springs City PD	63	0	63			X	63
Saugerties Town PD	23	8	31	31		X	
Saugerties Village Police Department					X		
Scarsdale Vg PD	40	0	40			X	40
Schenectady City PD	143	0	143			X	143
Schenectady County Sheriff	10	0	10			X	10
Schodack Town PD	9	7	16	16	X		
Schoharie County Sheriff	15	8	23			X	23
Schoharie Vg PD	0	10	10	10	X		
Schuyler County Sheriff	17	6	23	23	X		
Scotia Vg PD	13	0	13	13	X		
Seneca County Sheriff	32	8	40	40	X		
Seneca Falls Town PD	12	5	17	17	X		
Shandaken Town PD						X	
Shawangunk Town PD	6	9	15			X	15
Shelter Island Town PD	9	3	12			X	12
Sherburne Vg PD	0	7	7			X	7
Sherrill City PD	3	11	14	14	X		
Shortsville Vg PD	0	1	1			X	1
Sidney Vg PD	8	0	8	8	X		
Silver Creek Vg PD	5	3	8			X	8
Skaneateles Vg PD	2	11	13			X	13
Sleepy Hollow Vg PD	24	0	24			X	24
Sodus Point Vg PD	0	3	3	3	X		
Sodus Vg PD	1	0	1	1	X		
Solvay Vg PD	14	7	21			X	21
Somers Town Police Department						X	
South Glens Falls Vg PD	6	7	13	13	X		
South Nyack-Grand View PD	6	9	15	15	X		
Southampton Town PD	85	11	96			X	96
Southampton Vg PD	29	5	34			X	34
Southold Town PD						X	
Southport Town Police Department						X	
Spencer Town Police Department					X		
Spring Valley Vg PD	55	1	56			X	56
St Johnsville Vg PD	1	17	18	18	X		
St Lawrence County Sheriff	33	0	33	33	X		
St. Regis Mohawk Tribal Police Department					X		

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Steuben County Sheriff	40	4	44	44	X		
Stillwater Town PD	0	18	18	18	X		
Stockport Town PD	0	6	6	6	X		
Stony Point Town PD	25	4	29			X	29
Suffern Vg PD	24	7	31			X	31
Suffolk County Park Police	35	3	38			X	38
Suffolk County PD	2,414	0	2,414			X	2,414
Suffolk County Sheriff	268	0	268			X	268
Sullivan County Sheriff	36	0	36	36	X		
SUNY - Albany	40	0	40			X	40
SUNY - Binghamton	31	0	31	31	X		
SUNY - Buffalo	61	0	61			X	61
SUNY - Downstate Medical Center	33	0	33			X	33
SUNY - Stony Brook	67	0	67			X	67
SUNY - Upstate Medical Center	15	0	15			X	15
SUNY College At Alfred	12	0	12	12	X		
SUNY College At Brockport	16	0	16	16	X		
SUNY College At Buffalo	32	0	32			X	32
SUNY College At Canton	10	0	10	10	X		
SUNY College At Cobleskill	10	0	10	10	X		
SUNY College At Cortland	18	0	18	18	X		
SUNY College At Delhi	11	0	11	11	X		
SUNY College At Farmingdale	15	0	15			X	15
SUNY College At Fredonia	16	0	16			X	16
SUNY College At Geneseo	13	0	13	13	X		
SUNY College At Morrisville	12	0	12	12	X		
SUNY College At New Paltz	23	0	23	23	X		
SUNY College At Old Westbury	17	0	17			X	17
SUNY College At Oneonta	17	0	17	17	X		
SUNY College At Oswego	21	0	21	21	X		
SUNY College At Plattsburgh	14	0	14	14	X		
SUNY College At Potsdam	12	0	12	12	X		
SUNY College At Purchase	23	0	23			X	23
SUNY College At Utica/Rome	11	0	11	11	X		
SUNY College Of Optometry	6	0	6	6	X		
SUNY College-Env. Science and Forestry	9	0	9	9	X		
SUNY Maritime College					X		
Syracuse City PD	468	0	468			X	468
Syracuse University						X	

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Tarrytown Vg PD	32	0	32			X	32
Ticonderoga Town PD	7	6	13	13	X		
Tioga County Sheriff	32	2	34			X	34
Tompkins County Sheriff	41	0	41			X	41
Tompkins County Sheriff's Office						X	
Tonawanda City PD	28	0	28			X	28
Tonawanda Town PD	102	0	102			X	102
Troy City PD	125	0	125			X	125
Trumansburg Vg PD	0	13	13			X	13
Tuckahoe Vg PD	25	0	25			X	25
Tupper Lake Vg PD	9	1	10	10	X		
Tuxedo Park Vg PD						X	
Tuxedo Town PD	12	0	12			X	12
Ulster County Sheriff	57	15	72			X	72
Ulster Town PD	24	9	33			X	33
Utica City PD	158	0	158			X	158
Vernon Vg PD	1	10	11	11	X		
Vestal Town PD	33	0	33			X	33
Walden Vg PD	14	14	28			X	28
Wallkill Town PD	30	7	37			X	37
Walton Vg PD	4	11	15	15	X		
Wappingers Falls Vg PD	3	33	36			X	36
Warren County Sheriff						X	
Warsaw Vg PD	5	5	10	10	X		
Warwick Town PD	31	7	38			X	38
Washington County Sheriff	33	11	44	44	X		
Washingtonville Vg PD	13	5	18			X	18
Waterford Town and Vg PD	10	0	10			X	10
Waterloo Vg PD	8	7	15	15	X		
Watertown City PD	66	0	66			X	66
Watervliet City PD	26	0	26	26	X		
Watkins Glen Vg PD	4	11	15	15	X		
Waverly Vg PD	10	5	15	15	X		
Wayland Vg PD	1	6	7	7	X		
Wayne County Sheriff	53	12	65	65	X		
Webb Town PD	5	4	9	9	X		
Webster Town and Vg PD						X	
Weedsport Vg PD						X	
Wellsville Vg PD	10	10	20			X	20
West Carthage Vg PD	0	8	8			X	8

RFP# 22798 - Appendix O - List of LEA's

Agency Name	Full Time Officers	Part Time Officers	Total # Officers	SJS Users	SJS Agency	Non SJS Agency	Non SJS Users
Waterloo Vg PD	8	7	15	15	X		
Watertown City PD	66	0	66			X	66
Watervliet City PD	26	0	26	26	X		
Watkins Glen Vg PD	4	11	15	15	X		
Waverly Vg PD	10	5	15	15	X		
Wayland Vg PD	1	6	7	7	X		
Wayne County Sheriff	53	12	65	65	X		
Webb Town PD	5	4	9	9	X		
Webster Town and Vg PD						X	
Weedsport Vg PD						X	
Wellsville Vg PD	10	10	20			X	20
West Carthage Vg PD	0	8	8			X	8
West Seneca Town PD	66	0	66			X	66
Westchester Co Dept Pub Safety	262	0	262			X	262
Westfield Vg PD	5	6	11			X	11
Westhampton Beach Vg PD	13	6	19			X	19
White Plains City PD	192	0	192			X	192
Whitehall Vg PD	4	16	20	20	X		
Whitesboro Vg PD	6	3	9			X	9
Whitestown Town PD	7	5	12	12	X		
Willing Town Police Department						X	
Windham Town PD	3	11	14	14	X		
Wolcott Vg PD						X	
Woodbury Town PD	19	1	20			X	20
Woodridge Vg PD						X	
Woodstock Town PD	10	10	20	20	X		
Wyoming County Sheriff	30	10	40			X	40
Yates County Sheriff	25	11	36			X	36
Yonkers City PD	608	0	608			X	608
Yorktown Town PD	55	0	55			X	55
Yorkville Vg PD	4	10	14	14	X		
Youngstown Vg PD					X		

Total (w/out NYSP)	55,357	2,439	57,796	3,008	199	340	54,788
New York State Police	4,582	0	4,582	4,582	X		
Total (with NYSP)	59,939	2,439	62,378	7,590	214	340	54,788

CONTRACT MODIFICATION GUIDELINES

The Contractor shall submit all requests for price adjustments to add Products to the Contract in accordance with the Contract Modification Procedures below. The following guidelines are subject to change at the discretion of OGS. The Contract Modification Form to be used in connection with this process is included below, and is subject to change at the sole discretion of OGS.

A Contract Modification requires mutual agreement of the Contractor and the State, formalized in an executed document, to be provided by OGS Contract Administrator, after submission and approval of the Contract Modification Form.

A. Types of Contract Modifications: In order to expedite processing of a contract modification, where proposed changes involve more than one category below, each change should be submitted to OGS as a separate request.

(1) Updates: "Updates" are changes that do not require a change to the established Centralized Contract terms and conditions. Updates may include: Centralized Contract changes and updates made in accordance with the previously approved pricing formula (e.g. discount from list price); adding new products within the scope of the Contract and within the established, previously approved pricing structure; lowering pricing of products already on Contract, deleting products available through the Centralized Contract, adding products that do not fall under the previously established price structure or discounts under the Contract, re-bundled products, and other updates not listed above that are deemed to be in the best interest of the State and do not result in a change to the established Centralized Contract terms and conditions. Updates must be submitted to OGS for review, and must be accompanied by a justification of reasonableness of price if the change results in a change in pricing methodology. OGS will notify Contractor in writing if approved.

(2) Amendments: "Amendments" are changes that are not specifically covered by the terms and conditions of the Centralized Contract but inclusion is found to be in the best interest of the State. Requests for product changes and other requests that would require changes to the terms and conditions of the Centralized Contract would fall into the Amendments category. Contractor must provide a written justification of reasonableness of the price levels offered and a statement explaining why it is in the best interest of the State to approve the requested amendment. Amendments typically require negotiation between OGS and the Contractor. OGS will work directly with the Contractor to obtain the required documentation for each requested amendment and notify Contractor in writing if approved.

B. Contractor's Submission of Contract Modifications: In connection with any Contract modification, OGS reserves the right to:

- request additional information
- reject Contract modifications
- remove Products from Contract modification requests
- request additional discounts for new or existing Products

(1) Price Level Justification – Format: Contractor is required to submit the Product and price level information for the update in an Excel spreadsheet format electronically via e-mail (and in hard copy if requested by OGS) to the OGS Contract Administrator. The list must be dated. The Product and price level information should include and identify (e.g., by use of separate worksheets or by using italics, bold and/or color fonts):

- Price level increases
- Price level decreases
- Products being added

(2) Supporting Documentation: Each modification request must include the current contract pricing discount relevant to the Products included in the update.

(3) Submittal of Modification Requests: A Contract modification request must be accompanied by a completed Contract Modification Form. Contractor should briefly describe the nature and purpose of the update (e.g., update requested in order to reflect a recently approved GSA schedule, to restructure the price level to its customers generally, and/or for new Products which fall within the scope of the Contract). The Contract Modification Form must contain original signatures by an individual authorized to sign on behalf of Contractor and must be notarized.

STATE OF NEW YORK
 EXECUTIVE DEPARTMENT - OFFICE OF GENERAL SERVICES
 Corning Tower – 38th Floor
 Empire State Plaza
 Albany, New York 12242

CONTRACT MODIFICATION FORM	
OGS CONTRACT NO.: _____ CONTRACT DESCRIPTION: _____	DATE OF SUBMISSION: _____
CONTRACT PERIOD: From: _____ To: _____	VENDOR CONTACT: NAME: _____ PHONE NO: _____ E-MAIL: _____
<p>NOTE: Submission of this FORM does not constitute acceptance by the State of New York until approved by the appropriate New York State representative(s).</p>	

INSTRUCTIONS:

1. This form is to be used for all Contract modifications. The form is to be completed in full, signed and submitted to OGS for final approval. Any submission that is not complete and signed will be rejected.
2. Contractor is required to submit the Product and price level information for the update electronically via e-mail in either an Excel spreadsheet (and in hardcopy if requested by OGS) to the OGS Contract Administrator for this Contract.
3. Price level increase requests must be submitted in accordance with the Centralized Contract.
4. If more than one type of modification is being requested, each type should be submitted as a separate request.

The Contract modification request must be accompanied by the relevant contract pricing discount information.

COMPLETE STATEMENTS 1 THROUGH 5 BELOW:

<p>1. This request is for an: <input type="checkbox"/> Update <input type="checkbox"/> Amendment</p> <p>See Contract Modification Procedure for an explanation of these terms.</p>	<p>2. The intent of this submittal is to request: <input type="checkbox"/> Addition of new products or services <input type="checkbox"/> Deletion of products or services <input type="checkbox"/> Change in pricing level <input type="checkbox"/> Other Update <input type="checkbox"/> Other Amendment</p>
<p>3. All discounts are: <input type="checkbox"/> GSA <input type="checkbox"/> Most Favored Nation* <input type="checkbox"/> Other (provide explanation) _____</p> <p>*Prices offered are the lowest offered to any similarly situated entity.</p>	<p>4. Attached documentation includes: <input type="checkbox"/> Current approved GSA (labeled "For information only") <input type="checkbox"/> Current relevant Price List (labeled "For information only") <input type="checkbox"/> Revised NYS Net Price List in same format as found in the Pricing Appendix for this Contract <input type="checkbox"/> Current copy of the "National Consumer Price Index for All Urban Consumers (CPI-U) Northeast region" (for price increases only)</p>
<p>5. Describe the Nature and Purpose of the modification. If applicable, please explain how pricing has been structured to customers, and/or identify and describe new Products which fall into a new group or category that did not exist at the time of approval of the Contract by the Office of General Services.</p>	

The following CORPORATE ACKNOWLEDGEMENT statement must be signed by an individual authorized to sign on behalf of Contractor for the modification being requested in this Contract Modification document. The authorizing authority's signature must be notarized.

 Signature of Authorized Vendor Representative

CORPORATE ACKNOWLEDGMENT

STATE OF _____}; **ss.:**

COUNTY OF _____}

On the ____day of _____in the year 20__, before me personally came: _____, to me known, who, being by me duly sworn, did depose and say that he/she/they reside(s) in _____; that he/she/they is (are) _____ (the President or other officer or director or attorney in fact duly appointed) of _____, the corporation described in and which executed the above instrument; and that he/she/they signed his/her/their name(s) thereto by authority of the board of directors of said corporation.

Notary Public

OGS APPROVAL

Approved _____ Approved as amended _____ Disapproved _____

Name: _____

Title: _____ Date _____



Criminal Justice Information Services (CJIS) Security Policy

Version 5.2

8/9/2013

CJISD-ITS-DOC-08140-5.2



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	08/09/2013	APB & Compact Council

SUMMARY OF CHANGES

Version 5.2

1. In Executive Summary, paragraph two (2), add “data” second sentence – administrative change
2. In Executive Summary, paragraph four (4), add “(SIB)” to end of first sentence – administrative change
3. In Section 3.2.2(3)b, change “CJIS data” to “CJI” – administrative change
4. In Section 3.2.10, delete “a current ISO homepage on the Law Enforcement Online (LEO) network and” and “via the iso@leo.gov email address” and add “a security policy resource center (SPRC) on FBI.gov” – administrative change
5. In Section 3.2.11, add “or Chief Administrator” – APB approved change
6. In Section 4.1(4), add “when accompanied by any personally identifiable information.” – APB approved change
7. In Section 4.1 add “The following type of data is exempted from the protections levels required for CJI: Transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.” – APB approved change
8. In Section 4.1, final paragraph, add “released in the interest of public safety.” – APB approved change
9. In Section 5.1.1, final paragraph, add “Law enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI.” – APB approved change
10. In Section 5.1.1.3, change “CJIS data” to “CJI” – administrative change
11. In Section 5.1.1.6, first paragraph, change “CJIS data” to “CJI” – administrative change
12. In Section 5.1.1.6, second paragraph, change “CJIS data” to “CJI” – administrative change
13. In Section 5.1.1.6, second paragraph, change “...CSA/SIB...” to “...CSA, SIB, or authorized agency...” – APB approved change
14. Change title of Section 5.1.1.7 to read “Outsourcing Standards for Channelers” – APB approved change
15. Add new Section 5.1.1.8 Outsourcing Standards for Non-Channelers – APB approved change
16. In Section 5.1.2, add “authorized agency, or FBI” – APB approved change
17. In Section 5.1.2.1, add “authorized agency, or FBI” – APB approved change
18. Add new Section 5.1.4 Secondary Dissemination of Non-CHRI – APB approved change
19. Renumber previous Section 5.1.4 to 5.1.5 – administrative change
20. In Section 5.2.1.1, add “Social engineering” as a new item number nine (9) – APB approved change
21. In Section 5.2.1.1, move previous item number nine (9), “Dissemination and destruction”, to item number 10 – administrative change
22. In Section 5.2.1.2, delete item number seven (7), “Social engineering” – APB approved change
23. In Section 5.2.1.2, delete item number nine (9), “Media protection” – administrative change

24. In Section 5.3.1.1.1 delete “to all CSOs and ISOs through the use of the iso@leo.gov e-mail account” and add “via the security policy resource center on FBI.gov” – administrative change
25. In Section 5.4.1.1, modify language for clarification of requirements – administrative change
26. In Section 5.4.6, change “365 days” to “one (1) year” – administrative change
27. In Section 5.5.6.1, add “When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.” – APB approved change
28. In Section 5.5.7.3.1(1) add “as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.” – APB approved change
29. In Section 5.5.7.3.1(6) add “or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.” – APB approved change
30. In Section 5.5.7.3.1(7) add “or run a MDM system that facilitates the ability to provide antivirus services from the agency level.” – APB approved change
31. Add new Section 5.5.7.3.3 Mobile Device Management (MDM) – APB approved change
32. Renumber and rename previous section “5.6.2.1 Standard Authentication (Password)” to “5.6.2.1.1 Passwords” – administrative change
33. Change title of Section 5.6.2.1 to read “Standard Authenticators” – administrative change
34. In Section 5.6.2.1, add language for standard authenticators – administrative change
35. Add new Section 5.6.2.1.2 Personal Identification Number (PIN) – APB approved change
36. In Section 5.6.2.2.1, delete “For example,” – administrative change
37. In Section 5.6.2.2.1, change “2013” to “2014” for Interim Compliance, item number one (1) – APB approved change
38. In Section 5.6.2.2.1, add language to clarify advanced authentication (AA) – administrative change
39. In Section 5.6.2.2.1, change “2013” to “September 30, 2014” for Interim Compliance, item number two (2) (three (3) instances) – APB approved change
40. In Section 5.6.2.2.2(3)b, change “CJIS data” to “CJI” – administrative change
41. In Section 5.6.2.2.2(5), add “and located within” – administrative change
42. Rename Figure 8 to “Advanced Authentication Use Cases” – APB approved change
43. Replace Figure 8 example with use cases – APB approved change
44. In Figure 10 diamond #5, add “and located within – administrative change
45. In Figure 12, change “Advanced Encryption Standard (AES) 256” to “an encryption product that is FIPS 140-2 certified” – administrative change
46. In Section 5.9.1, change “5.9.1.9” to “5.9.1.8” – administrative change
47. In Section 5.9.1, change “2013” to “2014” for Physically Secure Location – APB approved change
48. Remove Section 5.9.1.8 Access Records – APB approved change
49. Renumber previous Section 5.9.1.9 to 5.9.1.8 – administrative change
50. Add new Section 5.10.1.5 Cloud Computing – APB approved change
51. In Section 5.10.3.2, change “Appendix G” to “Appendix G-1” – administrative change
52. Add definition of “Agency Controlled Mobile Device” to Appendix A Terms and Definitions – APB approved change

53. Add definition of “Agency Issued Mobile Device” to Appendix A Terms and Definitions – APB approved change
54. Add definition of “Cloud Client” to Appendix A Terms and Definitions – APB approved change
55. Add definition of “Cloud Computing” to Appendix A Terms and Definitions – APB approved change
56. Add definition of “Cloud Provider” to Appendix A Terms and Definitions – APB approved change
57. Add definition of “Cloud Subscriber” to Appendix A Terms and Definitions – APB approved change
58. In Appendix A Terms and Definitions, CJIS Systems Agency (CSA), change “CJIS data” to “CJI” – administrative change
59. In Appendix A Terms and Definitions, add language to Criminal Justice Information – APB approved change
60. Add definition of “Jailbreak (Jailbroken)” to Appendix A Terms and Definitions – APB approved change
61. Add definition of “Mobile Device” to Appendix A Terms and Definitions – APB approved change
62. Add definition of “Mobile Device Management (MDM)” to Appendix A Terms and Definitions – APB approved change
63. In Appendix A Terms and Definitions, Physically Secure Location, change “2013” to “2014” – APB approved change
64. Rename the title of Appendix A Terms and Definitions “Repository Manager” to “Repository Manager, or Chief Administrator” – APB approved change
65. Add definition of “Root (Rooting, Rooted)” to Appendix A Terms and Definitions – APB approved change
66. Add these acronyms to Appendix B: BYOD, MDM – APB approved change
67. Add this acronym to Appendix B: SPRC – administrative change
68. In Appendix C, paragraph four (4), change “CJIS data” to “CJI” – administrative change
69. In Appendix D-1, Part 1, item seven (7), change “CJIS data” to “CJI” – administrative change
70. In Appendix D-2, paragraph one (1), remove “Version 5, Sections 3.2.2 and 5.1” – administrative change
71. In Appendix D-2, paragraph one (1), add “, maintain,” – administrative change
72. In Appendix D-2, change paragraph two (2) to read, “...management control of the criminal justice function remains solely with the Criminal Justice Agency.” – administrative change
73. Rename Appendix F “IT Security Incident Response Form” to “Sample Forms” – administrative change
74. Add Appendix F-1 to “IT Security Incident Response Form” – administrative change
75. In Appendix F-1, remove personal email addresses – administrative change
76. Add Appendix G-3, Security and Access Subcommittee White Paper, Cloud Computing – APB approved change
77. Add Appendix G-4, Mobile Appendix – APB approved change
78. Add Appendix G-5, Personal Identification Number (PIN) – APB approved change
79. In Appendix H, 3.01, add “and all subsequent versions” – administrative change

80. In Appendix H, remove “2000” from “(2) The NCIC 2000 Operating Manual;” – administrative change
81. Add references to Appendix I – APB approved change
 - a. NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing
 - b. NIST Special Publication 800-145, The NIST Definition of Cloud Computing
 - c. NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations
82. In Appendix J, paragraph one (1), change “CJIS data” to “CJI” – administrative change
83. In Appendix J, 1.c., change title to “Outsourcing Standards for Channelers” – APB approved change
84. In Appendix J, 1.e., change title to “All Personnel (Security Awareness Training) – administrative change
85. In Appendix J, paragraph one (1) g, change “5.4.6 Audit Record Retention” to “5.4 Auditing and Accountability” – administrative change

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes.....	iii
Table of Contents	vii
List of Figures.....	xii
1 Introduction.....	1
1.1 Purpose.....	1
1.2 Scope.....	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document.....	2
1.5 Distribution of the CJIS Security Policy.....	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement.....	3
2.2 Architecture Independent.....	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO).....	5
3.2.3 Terminal Agency Coordinator (TAC).....	6
3.2.4 Criminal Justice Agency (CJA).....	6
3.2.5 Noncriminal Justice Agency (NCJA).....	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC).....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI).....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information.....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI.....	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information.....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information.....	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage.....	12
4.2.5 Justification and Penalties	12
4.2.5.1 Justification.....	12

4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services.....	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.1.5	References/Citations/Directives	19
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Awareness Topics	20
5.2.1.1	All Personnel.....	20
5.2.1.2	Personnel with Physical and Logical Access.....	20
5.2.1.3	Personnel with Information Technology Roles	21
5.2.2	Security Training Records.....	21
5.2.3	References/Citations/Directives	22
5.3	Policy Area 3: Incident Response	23
5.3.1	Reporting Information Security Events.....	23
5.3.1.1	Reporting Structure and Responsibilities.....	23
5.3.1.1.1	FBI CJIS Division Responsibilities	23
5.3.1.1.2	CSA ISO Responsibilities.....	23
5.3.2	Management of Information Security Incidents.....	24
5.3.2.1	Incident Handling.....	24
5.3.2.2	Collection of Evidence.....	24
5.3.3	Incident Response Training.....	24
5.3.4	Incident Monitoring.....	24
5.3.5	References/Citations/Directives	25
5.4	Policy Area 4: Auditing and Accountability.....	26
5.4.1	Auditable Events and Content (Information Systems).....	26
5.4.1.1	Events.....	26
5.4.1.1.1	Content.....	27
5.4.2	Response to Audit Processing Failures	27
5.4.3	Audit Monitoring, Analysis, and Reporting.....	27
5.4.4	Time Stamps.....	27
5.4.5	Protection of Audit Information.....	27
5.4.6	Audit Record Retention.....	27
5.4.7	Logging NCIC and III Transactions.....	28

5.4.8	References/Citations/Directives	28
5.5	Policy Area 5: Access Control.....	29
5.5.1	Account Management	29
5.5.2	Access Enforcement.....	29
5.5.2.1	Least Privilege	29
5.5.2.2	System Access Control	30
5.5.2.3	Access Control Criteria.....	30
5.5.2.4	Access Control Mechanisms.....	30
5.5.3	Unsuccessful Login Attempts	31
5.5.4	System Use Notification.....	31
5.5.5	Session Lock	31
5.5.6	Remote Access	32
5.5.6.1	Personally Owned Information Systems.....	32
5.5.6.2	Publicly Accessible Computers	32
5.5.7	Wireless Access Restrictions	32
5.5.7.1	All 802.11x Wireless Protocols	32
5.5.7.2	Legacy 802.11 Protocols.....	34
5.5.7.3	Cellular.....	34
5.5.7.3.1	Cellular Risk Mitigations.....	34
5.5.7.3.2	Voice Transmissions Over Cellular Devices	35
5.5.7.3.3	Mobile Device Management (MDM)	35
5.5.7.4	Bluetooth.....	35
5.5.8	References/Citations/Directives	37
5.6	Policy Area 6: Identification and Authentication	38
5.6.1	Identification Policy and Procedures.....	38
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	38
5.6.2	Authentication Policy and Procedures	38
5.6.2.1	Standard Authenticators.....	39
5.6.2.1.1	Password	39
5.6.2.1.2	Personal Identification Number (PIN)	39
5.6.2.2	Advanced Authentication.....	39
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	41
5.6.3	Identifier and Authenticator Management	43
5.6.3.1	Identifier Management.....	43
5.6.3.2	Authenticator Management.....	43
5.6.4	Assertions	43
5.6.5	References/Citations/Directives	44
5.7	Policy Area 7: Configuration Management	49
5.7.1	Access Restrictions for Changes	49
5.7.1.1	Least Functionality.....	49
5.7.1.2	Network Diagram.....	49
5.7.2	Security of Configuration Documentation	49
5.7.3	References/Citations/Directives	49
5.8	Policy Area 8: Media Protection.....	51

- 5.8.1 Media Storage and Access51
- 5.8.2 Media Transport51
 - 5.8.2.1 Electronic Media in Transit51
 - 5.8.2.2 Physical Media in Transit51
- 5.8.3 Electronic Media Sanitization and Disposal51
- 5.8.4 Disposal of Physical Media.....51
- 5.8.5 References/Citations/Directives52
- 5.9 Policy Area 9: Physical Protection53
 - 5.9.1 Physically Secure Location53
 - 5.9.1.1 Security Perimeter.....53
 - 5.9.1.2 Physical Access Authorizations53
 - 5.9.1.3 Physical Access Control53
 - 5.9.1.4 Access Control for Transmission Medium53
 - 5.9.1.5 Access Control for Display Medium53
 - 5.9.1.6 Monitoring Physical Access54
 - 5.9.1.7 Visitor Control54
 - 5.9.1.8 Delivery and Removal54
 - 5.9.2 Controlled Area54
 - 5.9.3 References/Citations/Directives54
- 5.10 Policy Area 10: System and Communications Protection and Information Integrity55
 - 5.10.1 Information Flow Enforcement55
 - 5.10.1.1 Boundary Protection55
 - 5.10.1.2 Encryption.....56
 - 5.10.1.3 Intrusion Detection Tools and Techniques56
 - 5.10.1.4 Voice over Internet Protocol.....56
 - 5.10.1.5 Cloud Computing.....57
 - 5.10.2 Facsimile Transmission of CJI.....57
 - 5.10.3 Partitioning and Virtualization57
 - 5.10.3.1 Partitioning.....57
 - 5.10.3.2 Virtualization58
 - 5.10.4 System and Information Integrity Policy and Procedures.....58
 - 5.10.4.1 Patch Management.....58
 - 5.10.4.2 Malicious Code Protection.....59
 - 5.10.4.3 Spam and Spyware Protection59
 - 5.10.4.4 Personal Firewall59
 - 5.10.4.5 Security Alerts and Advisories60
 - 5.10.4.6 Information Input Restrictions.....60
 - 5.10.5 References/Citations/Directives60
- 5.11 Policy Area 11: Formal Audits61
 - 5.11.1 Audits by the FBI CJIS Division.....61
 - 5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division61
 - 5.11.1.2 Triennial Security Audits by the FBI CJIS Division61
 - 5.11.2 Audits by the CSA.....61
 - 5.11.3 Special Security Inquiries and Audits61
 - 5.11.4 References/Citations/Directives61
- 5.12 Policy Area 12: Personnel Security63

5.12.1 Personnel Security Policy and Procedures63
 5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:..63
 5.12.1.2 Personnel Screening for Contractors and Vendors64
 5.12.2 Personnel Termination64
 5.12.3 Personnel Transfer.....65
 5.12.4 Personnel Sanctions.....65
 5.12.5 References/Citations/Directives65
Appendices..... A-1
Appendix A Terms and Definitions A-1
Appendix B AcronymsB-1
Appendix C Network Topology Diagrams C-1
Appendix D Sample Information Exchange Agreements..... D-1
 D.1 CJIS User Agreement D-1
 D.2 Management Control Agreement..... D-9
 D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding..... D-10
 D.4 Interagency Connection Agreement D-16
Appendix E Security Forums and Organizational Entities.....E-1
Appendix F Sample Forms.....F-1
 F.1 IT Security Incident Response Form F-2
Appendix G Best practices G-1
 G.1 Virtualization G-1
 G.2 Voice over Internet Protocol White Paper G-4
 G.3 Cloud Computing White Paper G-15
 G.4 Mobile Appendix G-30
 G.5 Personal Identification Number (PIN) G-51
Appendix H Security Addendum H-1
Appendix I ReferencesI-1
Appendix J Noncriminal Justice Agency Supplemental Guidance J-1
Appendix K Criminal Justice Agency Supplemental Guidance K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components.....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Implemented by a Local Police Department.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	25
Figure 6 – Local Police Department's Use of Audit Logs	28
Figure 7 – A Local Police Department's Access Controls	37
Figure 8 – Advanced Authentication Use Cases.....	44
Figure 9 – Authentication Decision for Known Location	47
Figure 10 – Authentication Decision for Unknown Location	48
Figure 11 – A Local Police Department's Configuration Management Controls	50
Figure 12 – A Local Police Department's Media Management Policies.....	52
Figure 13 – A Local Police Department's Physical Protection Measures.....	54
Figure 14 – A Local Police Department's Information Systems & Communications Protections	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	65

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent

policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJ. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Integrated Automated Fingerprint Identification System (IAFIS) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

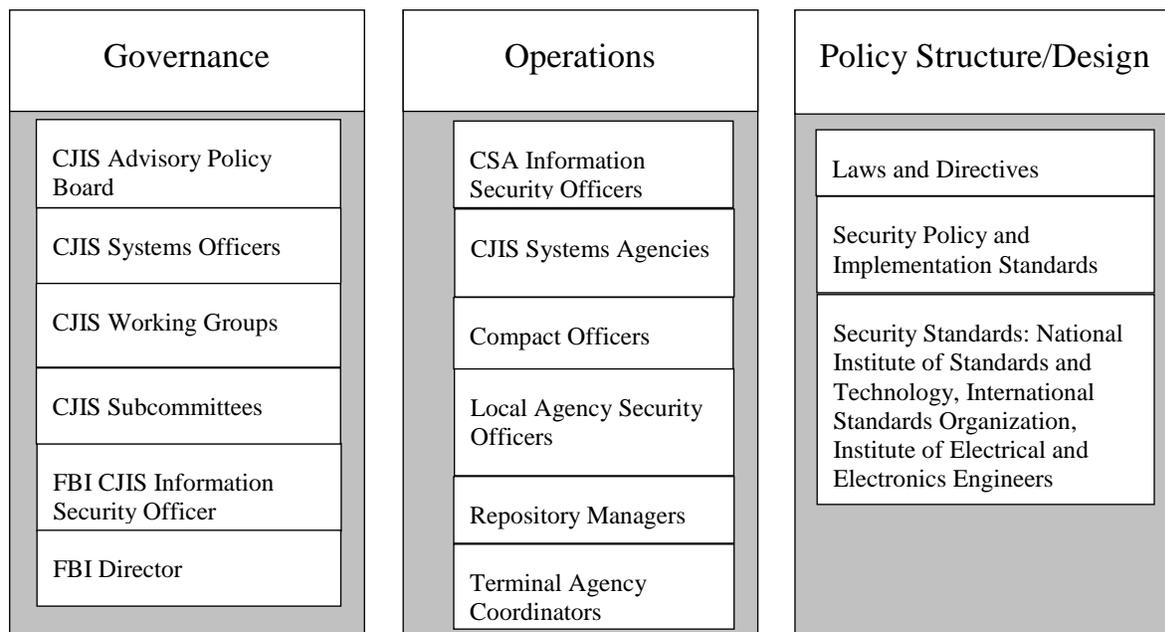


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJIS.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJIS, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
 - d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Approve access to FBI CJIS systems.
 - g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
 - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. **Identity History Data**—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. **Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. **Case/Incident History**—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files.
2. Known or Appropriately Suspected Terrorist Files.
3. Supervised Release Files.
4. Immigration Violator File (formerly the Deported Felon Files).
5. National Sex Offender Registry Files.
6. Historical Protection Order Files of the NCIC.
7. Identity Theft Files.
8. Protective Interest Files.
9. Person With Information (PWI) data in the Missing Person Files.

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other

government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record

for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the

standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJIS shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJIS. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or inter-agency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an inter-agency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall

be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 2640.2F.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney

General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the inter-agency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

5.1.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

5.2.1 Awareness Topics

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
2. Implications of noncompliance.
3. Incident response (Points of contact; Individual actions).
4. Media protection.
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Social engineering.
10. Dissemination and destruction.

5.2.1.2 Personnel with Physical and Logical Access

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.

5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.3 Personnel with Information Technology Roles

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.
3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB/Compact Officer. Maintenance of training records can be delegated to the local level.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 4 – Security Awareness Training Implemented by a Local Police Department

A local police department with a staff of 20 sworn law-enforcement officers and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

5.3 Policy Area 3: Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

5.3.1 Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document information system security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent

FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJIS was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts.
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;
 - b. modify the audit log file;

- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes,

for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

5.4.8 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of

rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.
3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. If encryption of stored information is employed as an access enforcement mechanism, the

cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see Section 5.10.1.2 for encryption requirements).

4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

- (i) the system use information is available and when appropriate, is displayed before granting access;
- (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
- (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is

unattended. A session lock is not a substitute for logging out of the information system. In the interest of officer safety, devices that are: (1) part of a police vehicle; or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.5.7.3 Cellular.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

5.5.7 Wireless Access Restrictions

The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below.

5.5.7.1 All 802.11x Wireless Protocols

Agencies shall:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
12. Disable all nonessential management protocols on the APs and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. Segregate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
15. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.5.7.2 Legacy 802.11 Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and are to be used only if additional security controls are employed.

Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.

1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
2. Enable WEP/WPA.
3. Ensure the default shared keys are replaced by more secure unique keys.
4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.

5.5.7.3 Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that employ cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.5.7.3.1 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication.
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information when session is terminated.
6. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

5.5.7.3.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

5.5.7.3.3 Mobile Device Management (MDM)

MDM facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery [if so desired by the agency].

Devices that have been rooted, jailbroken, or have had any unauthorized changes made to them shall not be used to process, store, or transmit CJI data at any time. In addition to the security controls described in this Policy, agencies shall implement the following controls when allowing CJI access from cell/smart phones and tablet devices:

1. CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration capable of at least:
 - i. Remote locking of device
 - ii. Remote wiping of device
 - iii. Setting and locking device configuration
 - iv. Detection of “rooted” and “jailbroken” devices
 - v. Enforce folder or disk level encryption

5.5.7.4 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.

The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption.

Agencies shall:

1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).
5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.
6. For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model. The "Just Works" model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to

secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.

9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
13. Establish a “minimum key size” for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.2 for minimum key encryption standards.
14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

5.5.8 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish

direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are the something you know, something you are, or something you have part of the identification and authentication process. Examples of standard authenticators include passwords, tokens, biometrics, and personal identification numbers (PIN). Agencies shall not allow the same authenticator (i.e., password, PIN) to be used multiple times on a device or system.

5.6.2.1.1 Password

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.2 Personal Identification Number (PIN)

Refer to Appendix G-5 Personal Identification Number (PIN) for FBI best practices for the use of PINs.

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, or "Risk-based Authentication" that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the

technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2014 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this Policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.
2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until September 30, 2014. Examples:
 - a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.
 - b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

- a. A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.
- b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assist decision makers in determining whether or not AA is required.

1. Can request's originating location be determined physically?
If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.
 - a. The IP address is attributed to a physical structure; or
 - b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.If neither (a) or (b) above are true then the answer is "no". Skip to question number 4.
2. Does request originate from within a physically secure location (that is not a police vehicle) as described in Section 5.9.1?
If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 3.
 - a. The IP address is attributed to a physically secure location; or
 - b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.
3. Are all required technical controls implemented at this location or at the controlling agency?
If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement waived.
 - a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
 - b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.If neither (a) or (b) above are true then the answer is "no". Decision tree completed. AA required.
4. Does request originate from an agency-managed user device?
If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 5.
 - a. The static IP address or MAC address can be traced to registered device; or

- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

- 5. Is the agency managed user device associated with and located within a law enforcement conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to question 6.

- a. The static IP address or MAC address is associated with a device associated with a law enforcement conveyance; or
- b. The certificate presented is associated with a device associated with a law enforcement conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a law enforcement conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Skip to question number 7.

- 6. Has there been an acquisition or upgrade since 2005?

If any of the (a), (b), (c), or (d) statements below are true the answer to the above question is “yes”. Proceed to question number 7.

- a. The “green-screen” MDTs have been replaced with laptops or other mobile devices; or
- b. An upgrade of technology exceeding 25% of the cost of the system being upgraded has taken place; or
- c. Any upgrade to the system encryption module has taken place; or
- d. Any upgrade to the system that is not replacing like technology has taken place.

If none of the (a), (b), (c), or (d) statements above are true then the answer is “no”. Decision tree completed. AA requirement waived.

- 7. Was IPSec implemented to meet the requirements of Policy Version 4.5?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA requirement is waived.

- a. The budget acquisition of IPSec was completed prior to January 1st, 2009 and IPSec was subsequently implemented; or
- b. Implementation of IPSec was completed prior to January 1st, 2009.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.
5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

5.6.5 References/Citations/Directives

Appendix C contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password (“something you know”), and a one-time password OTP (“something you have”) from a hardware token to satisfy the requirement for advanced authentication. Once the detective’s credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued

mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Figure 9 – Authentication Decision for Known Location

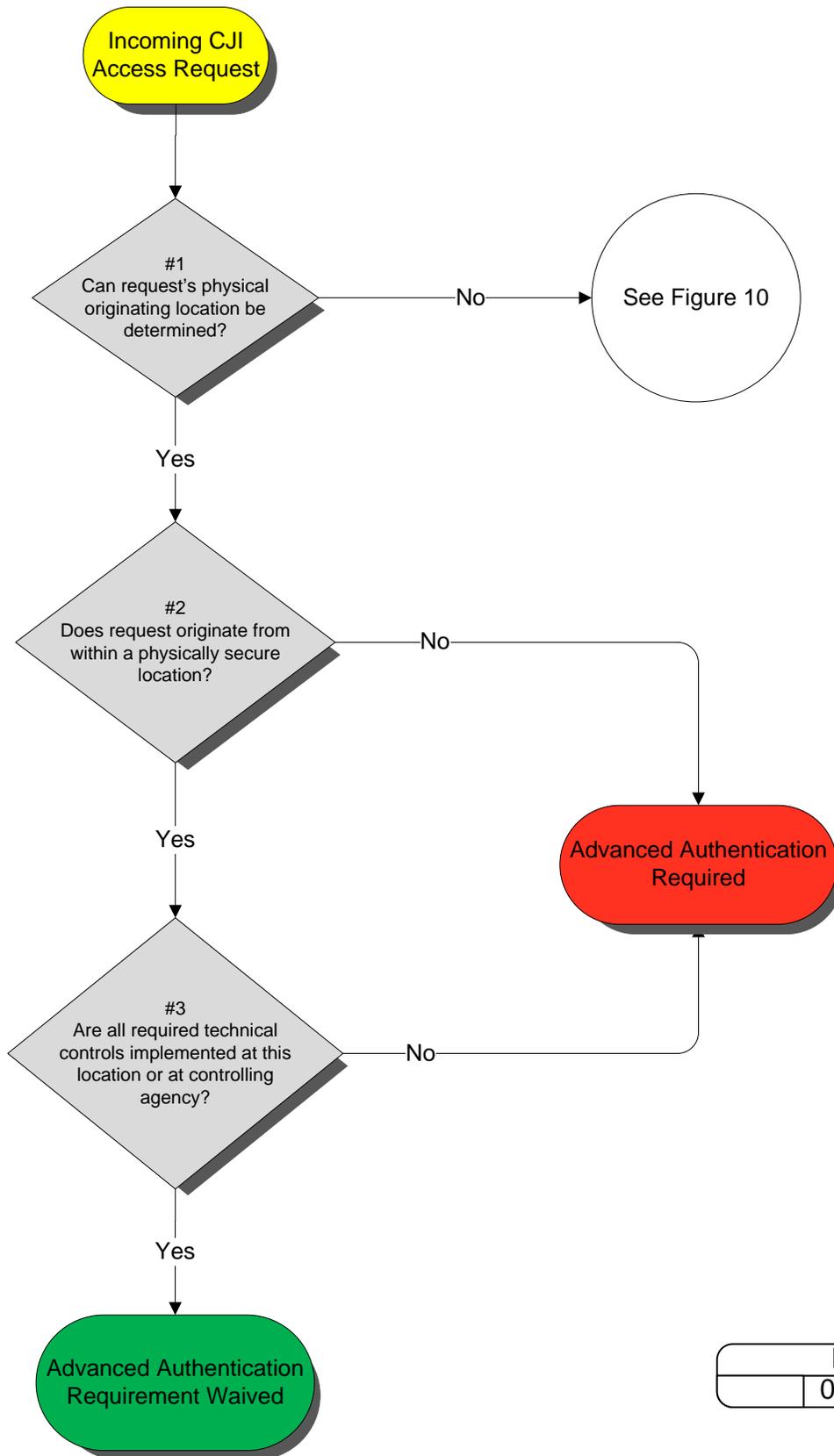


Figure 9		
	01/01/2011	

Figure 10 – Authentication Decision for Unknown Location

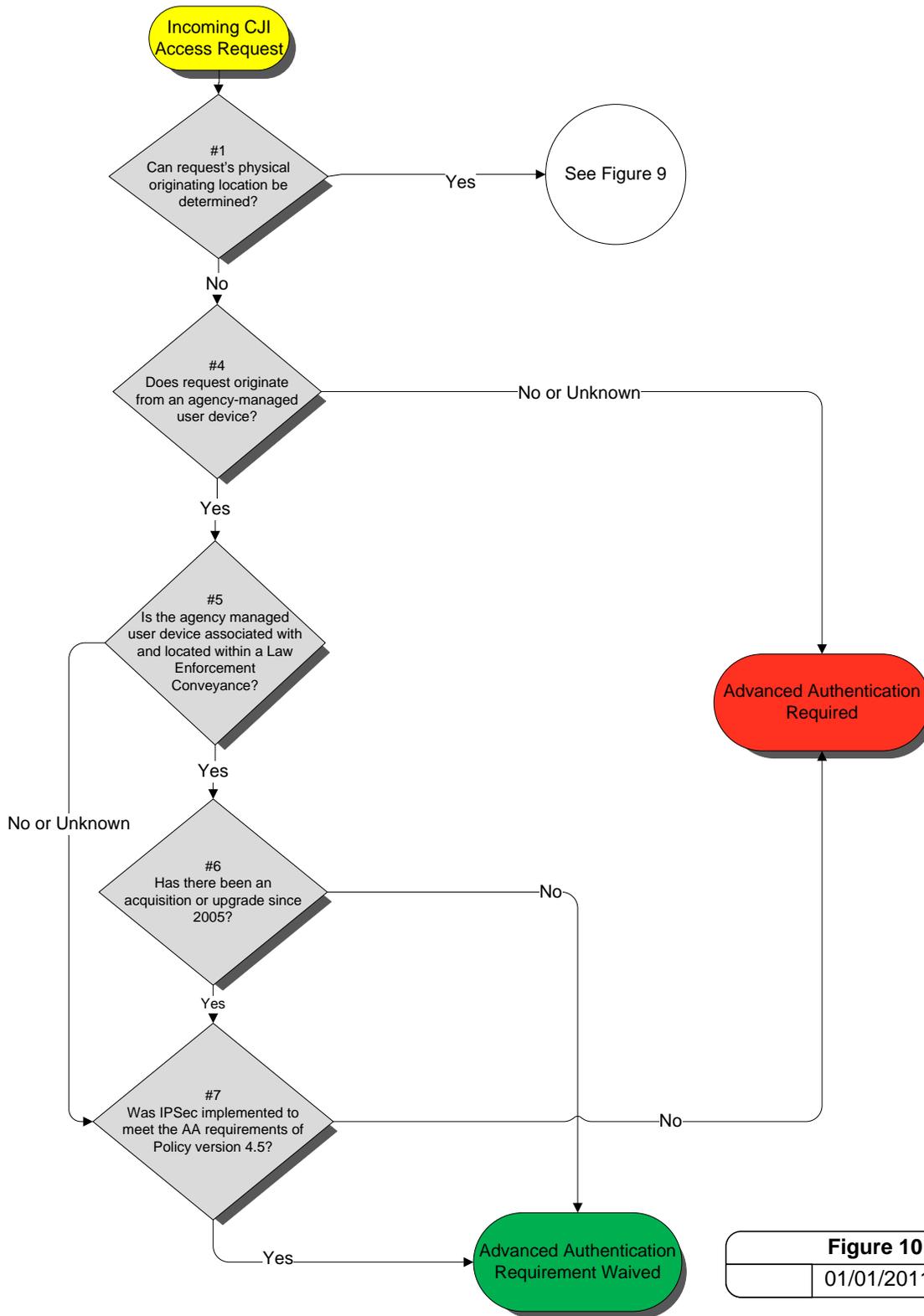


Figure 10		
	01/01/2011	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

5.7.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Electronic Media in Transit

“Electronic media” means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn’t possible then each agency shall institute other controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be

destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Section 5.6.2.2.1 describes the requirements for technical security controls required to access CJI within the perimeter of a physically secure location without AA.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2014. For the purposes of this Policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.

5.9.1.1 Security Perimeter

The perimeter of physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

5.9.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state’s CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by dispatchers, officers, and detectives. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems’ infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.10.4.4 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").
6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information

systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.

3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

5. For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:
 - a) Include authorization by a supervisor or a responsible official.
 - b) Be accomplished by a secure process that verifies the identity of the certificate holder.
 - c) Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone

services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via facsimile is exempt from encryption requirements.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services

(e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.
2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt

installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Personal Firewall

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this Policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.
2. Block unsolicited requests to connect to the user device.

3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

5.10.4.5 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.
5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.6 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

5.10.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 14 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJ, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJ shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Security Policy and Procedures

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - (i) 5 CFR 731.106; and/or
 - (ii) Office of Personnel Management policy, regulations, and guidance; and/or
 - (iii) agency policy, regulations, and guidance.

(See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
4. If a record of any other kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
5. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.

7. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI.
8. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.1.2 Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances.
2. If a record of any kind is found, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the Contractor-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

5.12.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of security the device potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI data.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: finger prints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Channeler — An FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJJ. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJJ. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtualized operating system.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Law Enforcement Online (LEO) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physically Secure Location — A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. For interim compliance, a police vehicle shall be considered a physically secure location until September 30th, 2014. For the purposes of this Policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — An IAFIS service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in

multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. Examples of acceptable documented evidence permitted to confirm an individual's state of residence are: driver's license, state or employer issued ID card, voter registration card, proof of an address (such as a utility bill with one's name and address as the payee), passport, professional or business license, and/or insurance (medical/dental) card.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEO	Law Enforcement Online
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle
MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency

NICS	National Instant Criminal Background Check System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PBX	Private Branch Exchange
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol

VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

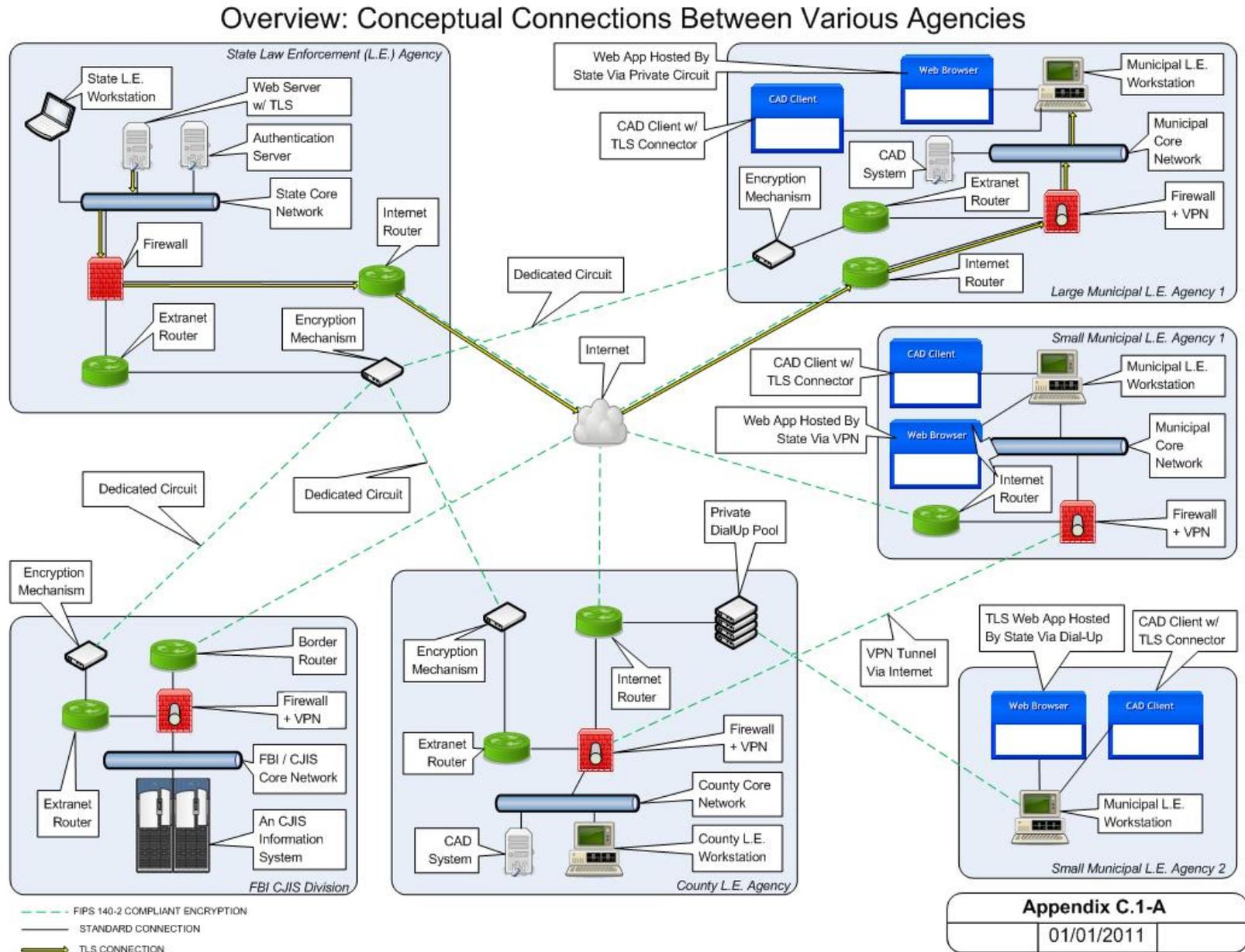
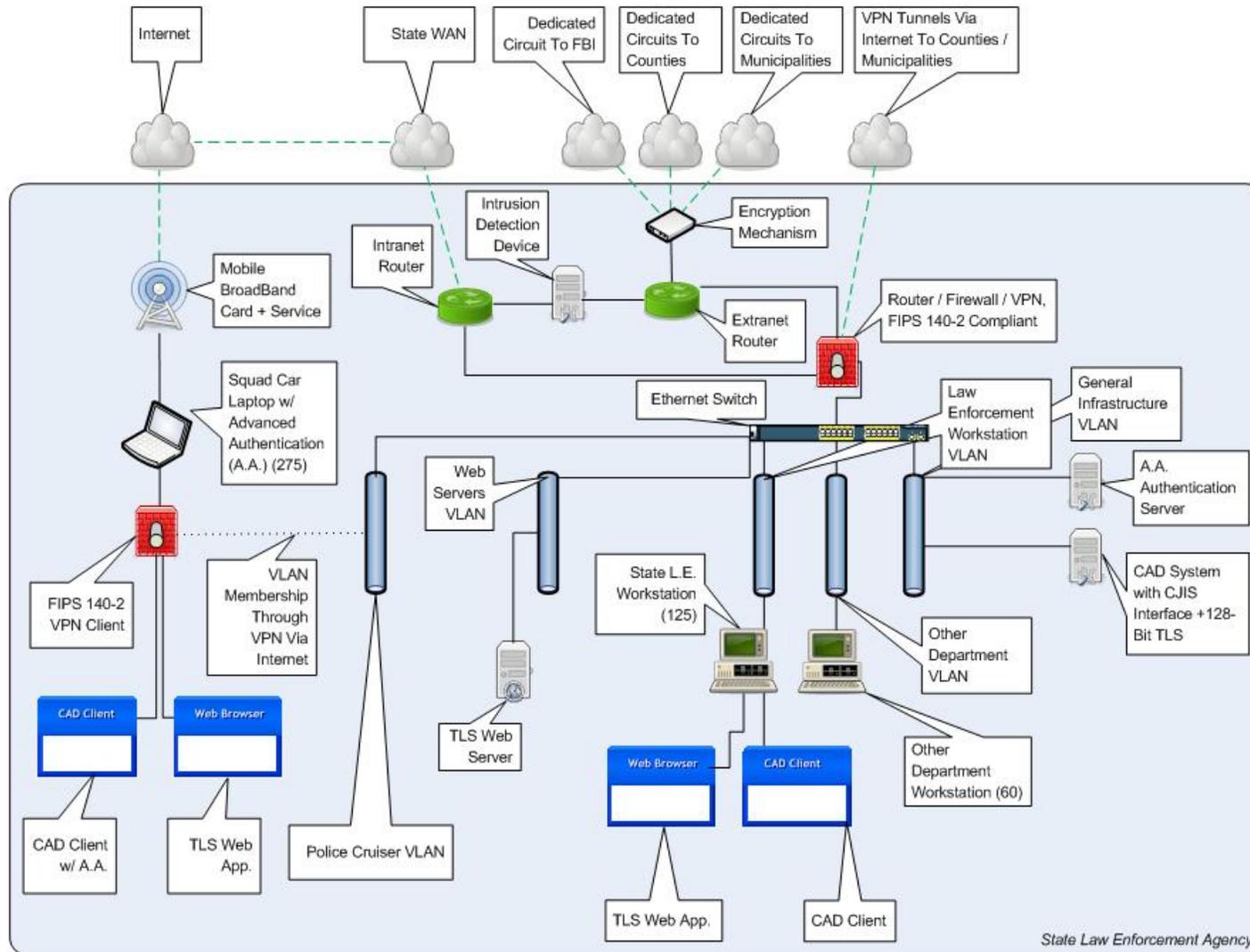


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

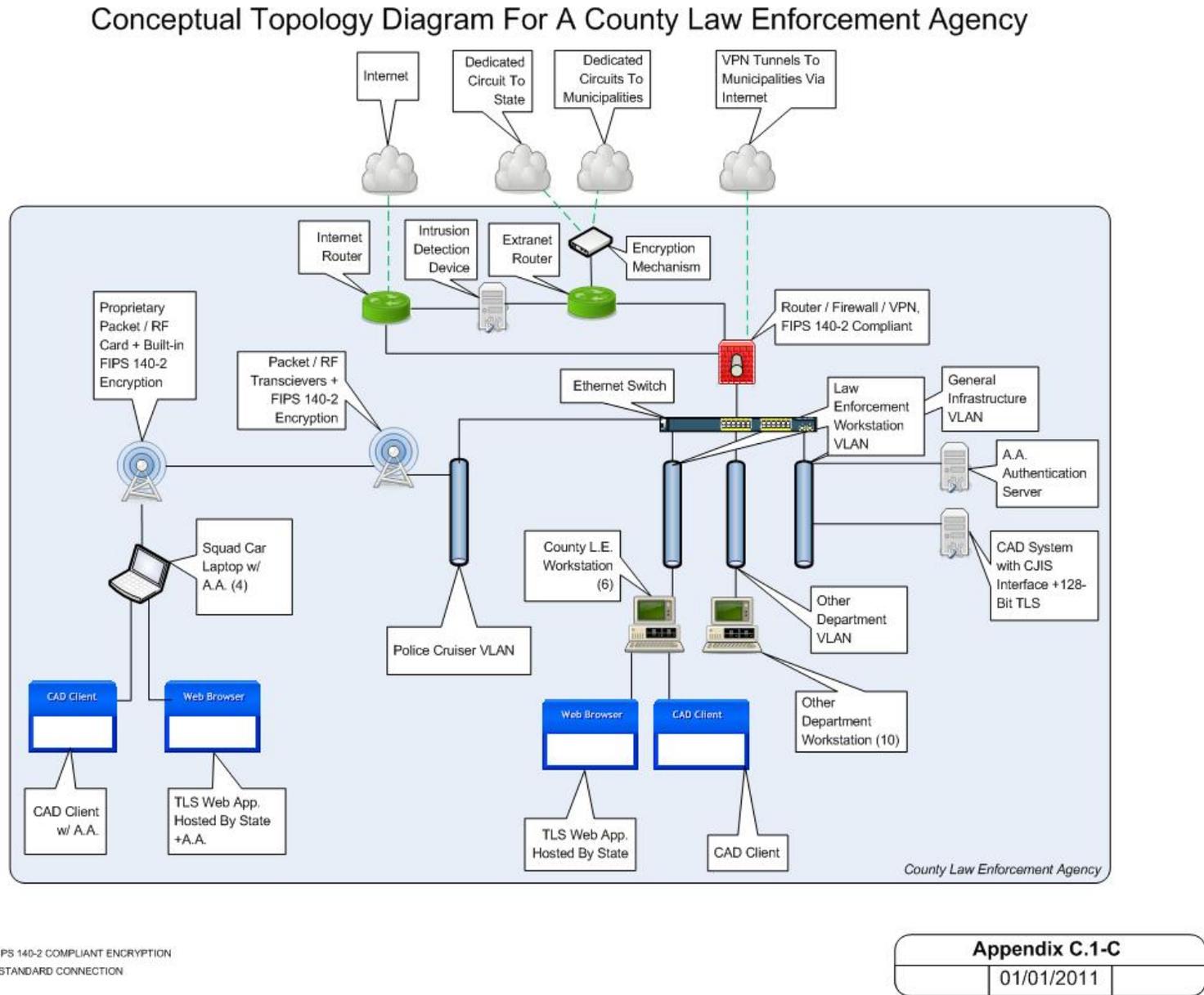
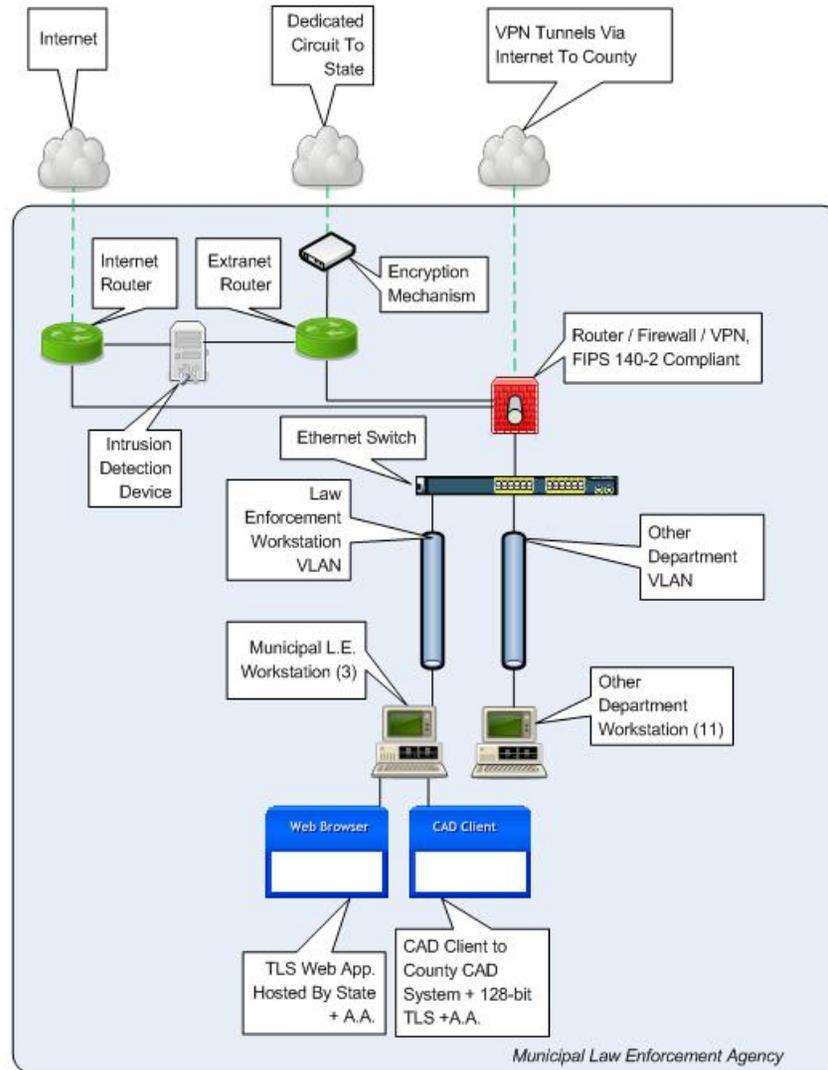


Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 ——— STANDARD CONNECTION

Appendix C.1-D		
	01/01/2011	

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEX); Law Enforcement Online; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history records. Additionally, each CSO must ensure that all agencies establish an

information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_____ Date: _____
CJIS Systems Officer

Printed Name/Title

CONCURRENCE OF CSA HEAD:
_____ Date: _____
CSA Head

Printed Name/Title

PART 2

_____ Date: _____
CJIS WAN Official (or other CJIS Authorized Official)

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:
_____ Date: _____
CJIS WAN Agency Head

Printed Name/Title

FBI CJIS DIVISION:

Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel.
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. **SECURITY:** It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. **AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:**

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. **FORCE AND EFFECT:** This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) Wide Area Network (WAN) USER AGREEMENT BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;

- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.
5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____
Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 IT Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

REPORTING FORM

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT: _____ PHONE/EXT/E-MAIL: _____

LOCATION(S) OF INCIDENT: _____

SYSTEM(S) AFFECTED: _____

METHOD OF DETECTION: _____

NATURE OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

George White

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-5849

iso@leo.gov

George White

(FBI CJIS CSIRC POC)

1000 Custer Hollow Road/Module D-2

Clarksburg, WV 26306-0102

(304) 625-5849

iso@leo.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

“Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure.”

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

“Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others.”

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

“Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *“Type-1 Hypervisor, which runs ‘bare-metal’ (on top of the hardware)*
- *“Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully support by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today account the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for SunxVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Vistual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide –area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virutalization.html>

<http://csrc.nist.gov/publications/drafts/6--=64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol White Paper

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer

using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic "CIA"). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch,

eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their

next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDICATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling.)
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use

cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures,

including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing White Paper

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

Ultimately, the move to cloud computing is a business decision in which the following relevant factors are giving proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CSP and also cloud compute?”

Because the CSP is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CSP.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CSP requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the CSP requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. The following questions can help frame the process of determining compliance with the existing requirements of the CSP.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy? (client or cloud service provider)
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)
- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle logging and provide that upon request?

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CSP, device and architecture independence can permit the use of cloud computing, but the security requirements do not change.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

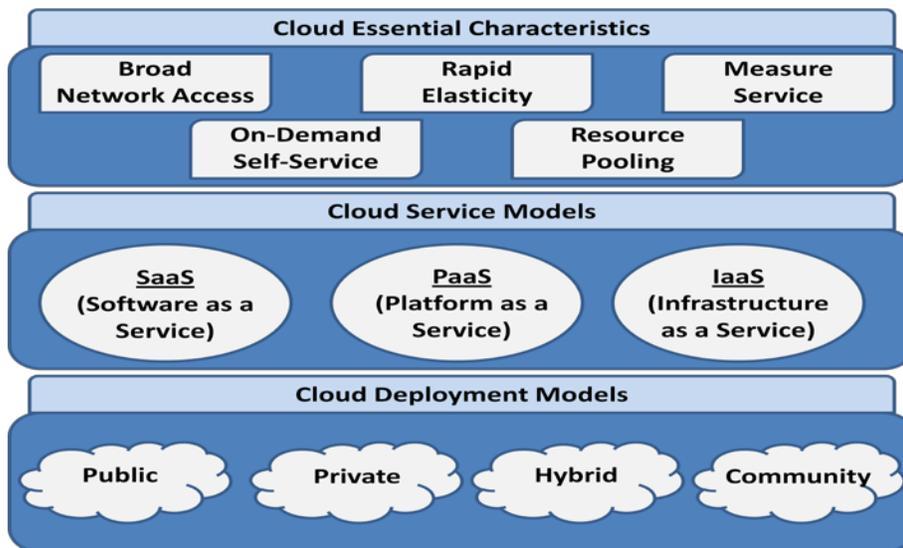


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the

organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to

prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can

impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	<ul style="list-style-type: none"> • Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	<ul style="list-style-type: none"> • Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	<ul style="list-style-type: none"> • Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	<ul style="list-style-type: none"> • Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	<ul style="list-style-type: none"> • Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software Isolation	<ul style="list-style-type: none"> • Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	<ul style="list-style-type: none"> • Evaluate the suitability of the cloud provider’s data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. • Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	<ul style="list-style-type: none"> • Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization’s continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.
Incident Response	<ul style="list-style-type: none"> • Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor to large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where

battery life and power efficiency are primary design drivers. This inherently limits the types of services that can function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. 'always on cellular' vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes 'on demand' cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations

either through the operating system or a third-party mobile device management (MDM) system may be able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by 'always on' network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with 'always on' cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as 'always on' or 'on demand'. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain 'airplane' mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other 'eavesdropping' devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a 'personal firewall' if properly configured and supported by a well designed organizational infrastructure. However, that equivalency does not apply to full featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an 'always on' cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes 'on-demand' cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or 'connected' to the cellular network. They connect to the network or internet through WiFi 'hotspots' or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJJ. Significant compensating controls may be needed to ensure devices accessing CJJ over 'public' WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with 'on-demand' cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking ('bricking') or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full featured laptops but may not be available for limited feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most 'smartphones'. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly

respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: "Is it reasonable to assume CJI could be accessed") as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a 'momentary' loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while 'minimal' durations might include a few minutes of time and 'extended' periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed.

However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full

function operating system. Therefore, the overall auditing design should take into account retrieval and consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be

modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device. Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. Facetime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the

device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from 'general user' access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of 'routine' device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

'Rooting' (Android OS) or 'Jailbreaking' (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of 'traditional' anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use.

Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a 'stock' Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with 'rooting' and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate 'secure' versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the 'internal' storage of the device, the Android OS does not provide secure separation of data stores on 'external' storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific 'external' media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via 'always-on' cellular data connections and the devices built-in GPS. Device tracking with WiFi only or 'on-demand' cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered when allowing BYOD employment. Device tracking is available for both limited

function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without 'always-on' cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from

accessing other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical

user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Personal Identification Number (PIN)

Personal Identification Number

Agencies should follow the PIN attributes, below, when a PIN is authorized for use in any identification and authentication process. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes is used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 180 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, **AND** the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 180 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, it should be a minimum of six (6) digits.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
- 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CJA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI), May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings
- [USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.6 – Agency User Agreements
 - c. 5.1.1.7 – Outsourcing Standards for Channelers*
 - d. 5.1.3 – Secondary Dissemination
 - e. 5.2.1.1 – All Personnel (Security Awareness Training)
 - f. 5.3 – Incident Response
 - g. 5.4 – Auditing and Accountability
 - h. 5.8 – Media Protection
 - i. 5.9.2 – Controlled Area
 - j. 5.11 – Formal Audits **
 - k. 5.12 – Personnel Security***

* Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

**Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

*** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication (web-site access)
 - c. 5.10.1.2 – System and Communications Protection – Encryption

4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity

5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
 - a. 5.7 – Configuration Management
 - b. 5.10 – System and Communications Protection and Information Integrity

6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA’s designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance is directed toward those criminal justice agencies that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJIS via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and, may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as “terminal agencies”. The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
 - a. 3.2.9 – Local Agency Security Officer (LASO)
 - b. 5.1.1.3 – Criminal Justice Agency User Agreements
 - c. 5.1.3 – Secondary Dissemination
 - d. 5.2.1.1 – Security Awareness Training
 - e. 5.3 – Incident Response
 - f. 5.4.6 – Audit Record Retention
 - g. 5.8 – Media Protection
 - h. 5.9 – Physical Security
 - i. 5.10.2 – Facsimile Transmission of CJIS
 - j. 5.11 – Formal Audits*
 - k. 5.12 – Personnel Security

*Note: States shall triennially audit all CJAs

2. When receiving CJIS via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
 - a. 5.5.2.4 – Access Control – Encryption
 - b. 5.6 – Identification and Authentication
 - c. 5.7 – Configuration Management
 - d. 5.10 – System and Communications Protection and Information Integrity