PIA
Printing Industries Alliance

September 7, 2018

Mr. Sean Carroll
Chief Procurement Officer, Council Chair
New York State Office of General Services
38th Floor, Corning Tower
Albany, NY 12242

Dear Mr. Carroll:

We are writing to provide additional input to the Procurement Council on the NYSID Application to become a Preferred Source for Digital Printing or as NYSID puts it, Mail Fulfillment. This input concerns a critical topic and is one that we believe has been given little consideration during this process. Data security is an important and expensive consideration for organizations producing digital printing, and their customers!

The development of digital printing technology enabled the combination of images and variable information (data) into a process that supports the production of a document that is truly unique to the recipient. This data can include elements such as name, address, phone number, email, date of birth, social security number, health information, names of family members, as well as, images, different colors, etc. To produce a digitally printed piece, the data elements need to be "delivered" to the production system that will be producing the printing. Generally, this "delivery" involves transmission to its production location via the internet. Of course, information of this nature is of prime interest to data hackers and cyber-criminals who will target either the originator or recipient of the data files. In the case of digital printing being done for a New York State agency, a prime target would be the particular printer charged with producing the work.

Government agencies are often the target for this activity by nature of the information residing in their database. It must also be noted that a data breach is not always caused by a hacker. In many instances they are mistakes caused by employee error, poor system design, etc. For example, the following are some of the largest data breaches affecting government entities from across the country in recent history:

- State of Texas (2011) – 3.5 million affected. Information lost included social security numbers, dates of birth and driver's license numbers.
- South Carolina Department of Revenue (2012) – 3.6 million affected. Information lost included social security numbers and credit/debit numbers.
- Tricare (2011) – 4.9 million affected. Information lost included full names, home addresses, phone numbers and social security numbers.
- Georgia Secretary of State Office (2015) – 6.2 million affected. Information lost included private information including social security numbers.
- Office of the Texas Attorney General (2012) – 6.5 million affected. Information lost included social security numbers.
- Virginia Department of Health Professions (2009) – 8.3 million affected. Information lost included patient records and prescriptions. A $10 million ransom was demanded for return of the information.
- U.S. Office of Personnel Management (2015) – 21.5 million affected. Information lost included federal personnel records.

PIA Headquarters
636 North French Road, Suite 1
Amherst, NY 14228
tel: 716-691-3211 or 800-777-4742
fax: 716-691-4249

NY/NJ Metro Office
195 Prospect Park West
Suite 1A
Brooklyn, NY 11215
cell: 203-912-0804

LI Office
3951 New York Avenue
Seaford, NY 11783
cell: 516-528-4747

www.PIAlliance.org | info@PIAlliance.org

Serving Graphic Communications Firms in New York State, Northern New Jersey and Northwestern Pennsylvania

- U.S. Department of Veteran Affairs (2006) – 26.5 million affected. Information lost included names, dates of birth and social security numbers. In 2009, the VA settled a $20 million lawsuit as a result.
- National Archives and Records Administration (2009) – 26 million affected. Information lost included highly sensitive information on a reported 26 million veterans.
- U.S. Voter Database (2015) – 191 million affected. Information lost included voter information (names, addresses, dates of birth, email addresses, party affiliation).

These are obviously the high profile data breaches that make the news and garner most of the public's attention. In most instances, the data breaches are smaller in scope but equally damaging in terms of expense and embarrassment. Ironically, the New York State Education Department, who regulates portions of the NYS Preferred Source program, was hit by a small but significant data breach earlier this year. In this instance, Questor Assessment, Inc., a SED vendor, experienced a data breach of students registered for computer-based testing in spring 2017. Of course, the SED breach is an example of a smaller incident that perhaps doesn't get the notoriety of the examples cited above but is more representative, but equally alarming, of what a typical state agency faces.

Data breaches, regardless of size, are embarrassing and costly to both the owner of the data and any vendor the data is entrusted to. Imagine the cost and political fallout if a New York State agency experienced a data breach of the magnitude of the occurrences referenced above and the repercussions for any staff or vendor involved! The previous examples have all been embarrassing for the governmental agencies involved and several have come with hefty price tags. The global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million with the average cost for each lost or stolen record containing sensitive and confidential information also increasing by 4.8 percent to $148 per record (Source: 2018 Cost of Data Breach Study by Ponemon).

Should the data breach involve information classified as protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), fines up to $1.5 million can be issued with the number multiplied by the number of years each violation has been allowed to exist.

Printing firms who operate in this market take a variety of safeguards to make sure that customer data they are managing is obtained in a secure fashion, is maintained securely while utilized and is disposed of in a secure fashion.

These actions encompass a wide variety of activities including:

Staff

- Make data and physical plant security a core business attribute
- Utilize strict written security protocols that are a condition of employment for all staff
- Regulate visitor and vendor access. All guests must be accompanied by employee escorts and properly authorized
- Security background checks are conducted on all employees
- All employees are bonded

Facilities

- Exterior doors are opened only with a valid security code
- Fire escapes and other doors not designed to be entered from the outside are equipped with alarms
- Key production areas are video and sight monitored 24/7

- Security partitions in production areas allow for deliveries and pick-ups without the need for visitors to access production area
- All Internet connections are protected by a firewall
- Extensive use of encryption is utilized for documents shared on an FTP site
- All incoming data is secured, processed and held for thirty days before deletion
- Adherence to strict operational procedures for system authentication, administration and data protection
- Regularly perform audits of systems and infrastructure for compliance with clients' procedures

The data security issue has been addressed extensively at the Federal level. The following information is a summary of the Federal Government Printing Office (GPO) standards and best practices:

Employees

The federal government requires vendors to have all employees meet or exceed the standards to Federal Public Trust Level Tier II (MBI) when potentially coming in contact with sensitive data.

Data Security

Qualified vendors should adhere to the following: federally recognized legislation, rules, and guidelines as applicable to the specific work:

- Federal Information Processing Standards (FIPS)
- Federal Information Security Act (FISMA)
- National Institute of Standards and Technology (NIST 800-53) guidelines
- SOC 2 Annual Assessment by a third party organization

Physical Security

Because print and mail, in this case, is a physical representation of confidential information, a variety of physical security measures are necessary in a facility where it is being produced.

Accountability

Qualified vendors should have a proven ability to adhere to the Federal guidelines for 100% Accountability of Production and Mailing." What this means is the vendor can provide a unique identifying number used to track each mail piece XXX validating the integrity of everything produced.

Capacity

Qualified vendors must not only meet the quality standards associated with Employees, Security, and Accountability, but must be able to meet these standards while handling large concentrated workflows.

State agencies handle data that is highly personal and of a sensitive nature. Because security mandates vary among these agencies, operating procedures and processes must address each agencies unique needs. Many firms regularly perform detailed audits to ensure compliance with customer requirements and recommendations in regulating production, storage, communications and other factors.

The vigorous auditing performed typically includes the following areas:

- Human Resources Screening and Statistics
- Training Procedures and Documentation
- Insurance, Legal and Liability Coverage
- Operational Workflow Controls
- Materials Management

- Policies, Standards and Procedures
- Management Reporting and Planning
- Access – Physical, Logical and Electronic
- Disaster Recovery Processes and Controls
- Authorization processes
- Environmental Controls
- Data Management procedures
- Contingency Planning

A variety of audits and auditor reports have been developed to test the security policies, procedures and protocols for organizations handling sensitive data. Examples include:

- Statements on Standards for Attestation Engagements (SSAE) #18
- Service Organization Control (SOC) reports (SOC 1, SOC 2, and SOC 3). There are also companies undergoing HIPAA audits that mirror audits performed by the United States Department of Health and Human Services. Office for Civil Rights.

These audit standards are developed by professional organizations, such as American Institute of CPAs. Cost for a SOC audit can range from $25,000 and go up from there. The costs to develop and implement these security protocols are very significant, running into the hundreds of thousands of dollars and up. Add to this the cost of the actual audits which start at $25,000 per year, the additional cost for cyber insurance and you get a good sense for the serious nature of the issue and the investment required for a printing company to operate in this market.

In summary, in addition to the arguments we have made previously on this issue, we believe that a serious examination should be made, by the Procurement Council, into the data security policies, protocols, staffing/training, and physical infrastructure of facility and IT systems of NYSID and the Center for Disability Services, prior to further considering this application.

Very truly yours,

Timothy Freeman
President, Printing Industries Alliance

cc: Mr. Thomas P. DiNapoli, NYS Comptroller
Ms. RoAnn Destito, Commissioner, NYSOGS
NYS Procurement Council
Interested Parties