

**United States
Consumer Product Safety Commission**



**Office of Inspector General
Audit of the CPSC Privacy Program**

December 18, 2009



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Memorandum

Date: December 18, 2009

TO : Inez Tenenbaum
Chairman

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Audit of the CPSC Privacy Program

The Office of Inspector General has completed its audit of the CPSC Privacy Program. A copy of the audit report is attached.

Management (EXIT, EXHR, ITIM, and EPDS) has been briefed regarding the findings and recommendations of this audit and given an opportunity to respond to them. Management's response may be found as an attachment to the audit report. Management concurred with most of the findings of the audit and agreed to implement corrective actions regarding these findings.

If, after reviewing the report, you concur with the findings and recommendations you may use the memorandum provided under separate cover to direct the Office of the Executive Director to implement the recommendations outlined in the audit report.

If you have any questions about this report or wish to discuss it, please feel free to contact me at 301-504-7644 or cdentel@cpsc.gov.

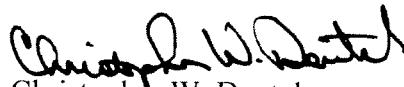

Christopher W. Dentel
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY

BACKGROUND	1
OBJECTIVE	1
RESULTS OF EVALUATION	1
RECOMMENDATIONS	2

INTRODUCTION 3

OBJECTIVE, SCOPE AND METHODOLOGY 5

RESULTS OF EVALUATION

Finding #1: Stolen CPSC laptop computers lacked encryption resulting in a potential loss of Privacy Act protected data	6
Finding #2: Risk of identity theft created by injury/investigation report attachments, posted on the CPSC intranet, that contain the personal information of injury victims	10
Finding #3: CPSC unable to verify security of records because privacy impact assessment reports have not been completed on all systems of records	11
Finding #4: Inadequate physical security over documents containing Privacy Act protected data	12
Finding #5: Inadequate training of employees regarding their responsibilities under the privacy program	14
Finding #6: Position descriptions of privacy program officials fail to reflect their duties related to privacy	17

COMMENTS TO REPORT

EXIT Comments	Attachment 1
EPDS Comments	Attachment 2
EXRM Comments	Attachment 3
ITIM Comments	Attachment 4

EXECUTIVE SUMMARY

BACKGROUND

The Federal Government requires appropriate information about its citizens to carry out the diverse missions mandated by the Constitution and laws of the United States. Long mindful of the potential adverse impact on individuals of the misuse of Federal records, the United States has adopted a comprehensive approach to limiting the Government's collection, use, and disclosure of personal information.

For example, the Privacy Act of 1974 requires that each government agency have in place an administrative and physical security system to prevent the unauthorized release of personal records. The act also states that that no agency shall disclose any record which is contained in a system of records by any means of communication to any person or to another agency except pursuant to a written request by, or with the prior written consent of, the individual to whom the records pertains, unless disclosure of the record would be to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties. The E-Government Act, among other things, enhances protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments, which are analyses of how personal information is collected, stored, shared, and managed in a federal system of records.

OBJECTIVE

This audit's objective was to review the Consumer Product Safety Commission's (CPSC) privacy program's documentation, policy, procedures, and implementation for compliance with appropriate regulatory guidance and statutes.

RESULTS OF EVALUATION

This report covers the commission's privacy program from fiscal year 2007 through fiscal year 2009 with emphasis on the privacy program's status as of June 30, 2009. Overall, we found that although the agency does have a functioning privacy program in place, that program has a number of weaknesses. Our findings included the following:

1. Stolen CPSC laptop computers lacked encryption resulting in a potential loss of Privacy Act protected data.
2. Risk of identity theft is being created by the posting of injury/investigation report attachments on the CPSC intranet that contain personal information from injury victims.
3. The CPSC is unable to verify the security of many of its records because privacy impact assessment reports have not been completed on all systems of records.
4. Inadequate physical security over documents containing Privacy Act protected data
5. Inadequate training of employees regarding their responsibilities under the privacy program
6. Position descriptions of privacy program officials do not reflect privacy related duties

RECOMMENDATIONS

To help the CPSC address the weaknesses identified above and strengthen its privacy program, we are providing the following recommendations:

1. Laptop computers issued to contractors for use in hospitals should have encryption and security software packages installed. In order to ensure that the contractors are complying with agency requirements regarding the physical security of laptop computers agency personnel should audit the physical security of laptop computers at hospital facilities. In order to further promote the physical security of these laptops the agency should consider installing tracking devices in them.
2. Privacy Act protected information should be redacted on injury investigation report attachments before they are posted on the CPSC intranet.
3. Privacy impact assessments (PIA) should be performed on all CPSC systems of records containing personally identifiable information (PII) that have not previously had PIAs performed on them to ascertain the security of said systems of records.
4. Procedures should be implemented to:
 - Secure documents containing privacy act protected data when they are not in use
 - Restrict access to file rooms that contain privacy act protected data through the use of combination or key locks
 - Check shredding containers that contain privacy act protected information (to ensure that they are not full or overflowing) at least bi-weekly.
5. Each office should conduct specialized privacy training for its employees and contractors who handle privacy information. This training must be relevant to the type of work that they perform and management should be required to retain documentation of said specialized training. Additionally, the general privacy training program should include quizzes to promote retention of the material covered and should generate training certificates for employees that complete privacy training.
6. The position descriptions for the Senior Agency Official for Privacy and the Privacy Advocate should be updated to include their duties related to the privacy program.

AUDITEE COMMENTS

The auditee responses have been included as attachments to this report. The auditees concurred with the majority of our findings and recommendations and indicated that work was already in progress to address many of the deficiencies found.

INTRODUCTION

Background: Privacy is a cherished American value, closely linked to our concepts of personal freedom and well-being. At the same time, fundamental principles such as those underlying the First Amendment, perhaps the most important hallmark of American democracy, protect the free flow of information in our society.

The Federal Government requires appropriate information about its citizens to carry out its diverse missions mandated by the Constitution and laws of the United States. Long mindful of the potential for misuse of Federal records on individuals, the United States has adopted a comprehensive approach to limiting the Government's collection, use, and disclosure of personal information.

Relevant Federal Statutes: There is no single federal law that governs all use or disclosure of personal information. Instead, U.S. law includes a number of separate statutes that provide privacy protections for information used for specific purposes or maintained by specific entities. The major requirements for the protection of personal information by federal agencies are set out in the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.

The Privacy Act requires that each government agency have in place an administrative and physical security system to prevent the unauthorized release of personal records. The act also states that that no agency shall disclose any record which is contained in a system of records by any means of communication to any person or to another agency except pursuant to a written request by, or with the prior written consent of, the individual to whom the records pertains, unless disclosure of the record would be to those officers and employees of the agency which maintain the record who have a need for the record in the performance of their duties.

The Privacy Act describes a “record” as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines a “system of records” as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system-of-records notice in the Federal Register that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended “routine” uses of data, and procedures that individuals can use to review and correct personally identifiable information.

The E-Government Act, among other things, enhances protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments, which are analyses of how personal information is collected, stored, shared, and managed in a federal system.

Privacy Program at the CPSC: As previously discussed, the Privacy Act mandates that each agency establish rules of conduct for persons involved in the design, development, operation or maintenance of any system of records, or in maintaining the records and instruct each such person with respect to such rules and requirements of the Privacy Act, including any other rules and procedures adopted pursuant to the Privacy Act and the penalties of non-compliance. OMB Memorandum M-07-16, Safeguarding Against and Responding to Breach of Personally Identifiable Information (PII), requires that agencies train their employees on their privacy and security responsibilities before providing them access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided that is commensurate with any increased responsibilities or changes in duties. CPSC Directives 760.1 and 1435.1 are the most relevant agency regulations in this area.

CPSC Directive 760.1 defines personally identifiable information (PII) as information that identifies an individual (e.g. name, address, social security number or other identifying number of code, phone number, email address) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e. indirect information. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptions which are linked to an individual.

CPSC Directive 1435.1 requires that the Senior Agency Official for Privacy (SAOP) provide policy guidance for and coordinate and oversee administration of the Commission's Privacy Program to ensure compliance with policies and procedures in the Privacy Act and OMB Circular A-130, Management of Federal Information Resources. Specifically, it sets out the following responsibilities for the SAOP:

The SAOP should ensure that the privacy program is periodically reviewed by the Inspector General;

The SAOP has oversight responsibility for implementation of the commission's privacy program;

The SAOP shall plan and conduct training, consistent with the requirements of the privacy act for all employees;

The SAOP should request specialized training, in addition to the required annual privacy training, for those individuals having primary responsibility for implementing the commission's privacy program; and

The SAOP shall oversee the day-to-day activities of the Commission's Privacy Program.

OBJECTIVE, SCOPE, METHODOLOGY

Objective

This audit's objective was to review the CPSC privacy program's documentation, policy, procedures and implementation for compliance with both agency regulations and general Federal Government's requirements such as the Privacy Act and the E-Government Act.

Scope

This audit evaluated the CPSC's privacy program for fiscal years 2007, 2008, and 2009 with emphasis on the state of the privacy program as of the completion of field work on this audit, June 2009.

Methodology

This evaluation was conducted in accordance with generally accepted government auditing standards. Field work was performed from December 2008 to June 2009 at the CPSC's headquarters in Bethesda, Maryland. To accomplish our objective, we reviewed policies and procedures, interviewed employees and obtained supporting documentation. We evaluated the CPSC's current privacy program and performed procedures necessary to test the adequacy of the privacy security controls. The principle criteria used for the review included:

Privacy Act of 1974 (5 U.S.C. 552a)

The E-Government Act of 2002 (Public Law 107-347) Title III, Federal Information Security Management Act of 2002 (December 17, 2002)

OMB Circular A-130 Revised Transmittal #4, Management of Federal Information Resources (11/28/2000)

OMB Circular A-19, Procedures for Coordination and Clearance by OMB of Agency Recommendations on Legislation (September 1979)

OMB Memorandum M-06-16, Protection of Sensitive Information (June 2006)

OMB Memorandum M-06-15, Safeguarding PII (May 2006)

OMB Memorandum M-07-16, Safeguarding Against and Responding to Breach of PII (May 2007)

OMB Memorandum M-03-22, OMB Guidance for Implementing Privacy Provisions of E-Gov Act (September 2003)

CPSC Directive 1435.1, Privacy Program Policy and Procedures (Revised 9/25/2007)

CPSC Directive 1435.6, Privacy Impact Assessment Policy (September 2007)

CPSC Directive 1450.2, Clearance Procedures for Providing Information to Public (January 2003)

We reviewed the adequacy of the agency's privacy training program in general with a special emphasis on determining whether the agency was providing the additional specialized training on privacy called for in recent OMB guidance. We followed up on reports of missing notebook computers that may have contained privacy information. We examined Epidemiologic Investigation Reports (Form 182) and attachments to determine if Privacy Act protected information was being inappropriately shared across the agency. As part of our review, we conducted a survey of the systems of records maintained at the agency. We reviewed the privacy impact assessment process to determine whether the CPSC had performed assessments on all systems of records containing privacy information. Additionally, we conducted on-site inspections of offices that handled documents containing privacy act protected information to observe if said documents were being appropriately secured.

RESULTS OF EVALUATION

Summary: Overall, we found that the agency has a privacy program that is in compliance with the majority of statutory and regulatory requirements. The program is implemented in the Office of Information Technology (EXIT) but administered differently in each of the offices we reviewed (Office of Hazard Identification and Reduction (Epidemiology, EPDS), Office of Human Resources (EXRM), Division of Information Management (ITIM), Equal Employment Opportunity Office (EEO) and Office of General Counsel (OGC)).

A number of findings were made regarding areas where the agency either failed to comply with CPSC specific and/or general Federal requirements or where qualitative improvements could be made in the privacy program.

Finding #1: Stolen CPSC laptop computers lacked encryption resulting in a potential loss of Privacy Act protected data

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, states that an agency should implement security requirements including the use of appropriate encryption. M-07-16 also states that agencies must report all incidents involving the breach of PII to the United States Computer Emergency Readiness Team (US-CERT). The requirement doesn't distinguish between potential and confirmed breaches.

The CPSC policy on safeguarding against and responding to the breach of PII states that law enforcement, OIG and US-CERT must be notified immediately when there is a theft of hardware that may contain PII. (Detection and analysis category B., Intentional Incident where data was not the target, but involving PII)

OMB Memorandum M-06-16 states that all data on mobile computers should be encrypted.

Several IT security incidents, including the theft of two CPSC laptop computers, occurred at the Directorate for Epidemiology's National Electronic Injury Surveillance Systems (NEISS) field sites between FY 2006 and FY 2009. (NEISS consists of statistically selected hospitals that report consumer product related emergency room injury visits to the CPSC daily.) These incidents involved the physical security of four notebook personal computers that were stolen, destroyed, or lost.

Of the four laptop computers:

- Two were stolen—One from a house and one from a car
- One was lost in the mail
- One was destroyed in a house fire

These CPSC laptop computers were used by NEISS coders (contractors, not Government personnel). A coder enters injury data from hospital forms. This data relates to emergency room visits related to injuries caused by consumer products. This data may include PII, such as the name, address and phone number of the patient, in order to allow Epidemiology personnel to “follow-up” with the patient. This information is converted into DOS ASCII text as soon as the information is entered into the laptop computer and saved. It is then uploaded by the Epidemiology software program installed in the computer and transmitted, via the hospital phone line, every night to the CPSC headquarters where the information is downloaded and processed into searchable text.

At the time of the field work, the Information Technology (IT) specialist interviewed stated that the laptop computers sent to hospitals were not encrypted with the CPSC Guardian Edge encryption software and did not use the CPSC security package software (which consists of anti-virus, patch management, anti-spyware, and firewall software). Additionally, there is no guarantee that the coders are securing their CPSC issued computers with the CPSC supplied cable lock.

Several months later, at the time of the drafting of this report, half of the NEISS laptop computers were transmitting accident data via appropriate internet secure socket encryption. The remaining half of the NEISS laptop computers were still using DOS ASCII encryption (which is not one of the approved forms of encryption) and transmitting data to CPSC via the phone line. According to the Information Systems Security Officer and the Inspector General, the theft of the two laptop computers was not reported to the Inspector General. However, they were reported to local law enforcement authorities, US-CERT, and the NEISS program office.

Additionally, the 17 laptop computers used by contractors to conduct Computer Assisted Telephone Interviews (CATI), follow-up telephone interviews that are conducted to supplement NEISS incident data, are not encrypted nor is there any guarantee that the contractors are physically securing their CPSC issued laptop computers.

We found, through discussion with Epidemiology management, that there is no verification that laptop computers distributed to hospitals and CATI contractors are physically secured at all times. The project manager stated that the security of the laptop computers is not one of the items verified by NEISS or contractor personnel when they visit the hospitals. The system owner and the Information Systems Security Officer (ISSO) did not feel it was necessary to encrypt data and install the CPSC standard security package on the computers issued to NEISS contractors since the NEISS data is encrypted into ASCII text as soon as it is entered into the computer and the CATI laptop computers do not contain privacy information.

Even though the loss of PII described above (loss of control over four computers) has not resulted in any known harm to the individuals impacted, it has put them at risk for identity theft and similar problems. Also, the CPSC incurred monetary loss when it had to replace the computers in question.

Recommendations: To address the problems identified above, the following 5 steps should be taken:

1. Develop and implement procedures requiring that laptops issued to contractors that contain NEISS data be secured via cable lock or similar means at all times;
2. All computers issued to contractors for use at/with NEISS hospitals should have their data encrypted in one of the approved formats and the security software ordinarily installed on CPSC computers issued to Government personnel should be installed on computers issued to contractor personnel;
3. Develop and implement procedures to ensure that when CPSC personnel visit NEISS hospitals to review the performance of the NEISS contractor personnel they also verify that contractors are complying with the above described procedures;
4. Management should ensure that contractor compliance with the above described physical security and data security requirements is mandated in the statement of work for NEISS hospital contracts;
5. Management should consider installing tracking devices in the personal computers used at the hospitals.

Auditee's Response to Recommendations:

EPDSC stated that NEISS coders do not conduct follow-up investigations but may provide privacy type information such as the name, address, and phone number of patients to EPDSC for further investigations by CPSC field staff or CATI contractors.

EPDSC stated that as of November 4, 2009 over 80% of the NEISS laptop computers have been switched to a new communications program with hard disk encryption, anti-virus software, and patch management.

EPDSC stated that in the draft audit report it was not clear that EPDS had reported the theft of the two laptop computers that were stolen on 12/31/2005 and 2/27/2008 through the appropriate channels at the CPSC.

EPDSC stated that the portion of the draft audit report that refers to NEISS laptop computers not handling privacy information was incorrect since these laptop computers do handle privacy information.

EPDSC stated that they have already made a significant amount of progress towards addressing the recommendations in the report.

ITPP's response to the first finding was that all contractor computers are configured to include encryption and security software.

OIG's Comments on Auditee's Responses to Recommendations:

We have changed the wording in this finding to clarify that NEISS coders do not conduct follow-up investigations.

At the time of the field work, we were told that the NEISS laptop computers did not have the new communications program or the new security programs installed. We stated that half of the NEISS laptop computers were transmitting accident data via the internet secure socket encryption as of the report draft date.

The draft audit report was modified to reflect that EPDSC did contact law enforcement and the ISSO. In turn, the ISSO did contact US-CERT. However, the IG was not contacted.

We revised the audit report to state that information is encrypted into ASCII text as soon as it is entered and that CATI laptop computers do not handle privacy information.

To address ITPP's comment on the contractor computers being "configured to include encryption and security software", we note that we did not find this to be the case during field work and that (at the time of this report) EPDSC had indicated they have not yet encrypted and secured all of the laptop computers in question.

Finding #2: Risk of identity theft created by injury/investigation report attachments, posted on the CPSC intranet, that contain the personal information of injury victims

The Privacy Act states that each agency must have in place an administrative and physical security system to prevent unauthorized release of personal records.

A search of the CPSC intranet using specific key words resulted in our locating 10 epidemiology injury/investigation reports (CPSC Form 182) and related attachments, and 1 public complaint displaying PII of injury victims. Six of the ten investigation reports were dated after January 15, 2009 and had attachments that contained Privacy Act Protected information. The program manager of the Division of Data Systems sent an email on January 15, 2009 directing data systems personnel to purge privacy data before it was scanned into the field investigation database. On three of the eleven records, a death certificate was attached with a social security number.

At the request of the Office of Inspector General, The Office of General Counsel issued the following opinion on privacy data on April 3, 2009.

Regardless of the legal right of the agency, it is CPSC policy that the privacy of an individual is a personal and fundamental right that shall be respected and protected. CPSC Order 1435.1, Policies and Procedures Pursuant to the Privacy Act, dated September 25, 2007. Furthermore, because the loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience and may lead to identity theft or other fraudulent use of the information, Federal agencies have a special duty to protect that information from loss or misuse. See OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, dated May 22, 2006. Therefore, if the presence of the SSN in the Reports is not relevant and necessary to accomplish a lawful agency purpose, the SSNs should be redacted prior to publication of the Reports on the agency intranet.

The cause of the privacy information being accessible to all CPSC staff is that Division of Data Systems staff are not complying with the requirement to purge privacy data in their database.

The effect of this problem is that the PII of victims (such as names, addresses, phone numbers and social security numbers) is visible to all users of the CPSC intranet. This creates a risk of identity theft and represents a failure to adequately protect personal information covered by the Privacy Act.

Recommendations: Staff should delete privacy data that is not relevant and necessary to accomplish a lawful agency purpose. Specifically, in this case the SSNs and any other personally identifiable information that is not relevant and necessary should be redacted before investigation reports and attachments are scanned into the website. Additionally, staff should also delete such information from old records.

Auditee's Response to Recommendations

ITPP has indicated that they have identified a technical solution and are in the process of implementing it; but have not provided a timeline of when implementation will occur.

EPDS has, correctly, indicated that not all personally identifiable information is covered by the relevant prohibition, only such personally identifiable information as is "not relevant and necessary to accomplish a lawful agency purpose."

OIG's Comments on Auditee's Response to Recommendations:

The Finding and Recommendation have been changed to reflect that only social security numbers and any other personally identifiable information "not relevant and necessary to accomplish a lawful agency purpose" should be deleted, not all personally identifiable information.

Finding #3: CPSC unable to verify security of records because privacy impact assessment reports have not been completed on all systems of records

According to the CPSC Directive 1435.6, the Privacy Impact Assessment (PIA) Policy has been instituted in order to ensure that the systems of records the CPSC develops protect individuals' privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design. A PIA is required to be completed for new systems of records and systems under development or undergoing major modifications. Under current agency policy, a system of records does not have to undergo PIA review unless it is the subject of major modification or if automation or upgrading of the system puts data at risk.

The privacy impact assessment report contains the name of the system, a description of the system, type of data collected, attributes of the data, maintenance and administrative controls and access to controls.

As of June 12, 2009 only 12 privacy impact assessment reports had been completed. There are at least 20 existing systems of records and other PII inventoried type systems, such as the Federal Financial System and the HR Staffing Cases Files, that contain privacy type data.

The cause of this finding is that the Privacy Advocate is still in the process of reviewing the existing CPSC systems of records. The Privacy Advocate reports that she will be able to assess the situation in greater detail after the system of records review is finalized. The PIA procedure is only a few years old and has so far only included new systems and not existing systems.

The effect of the finding is that the agency doesn't know if there are adequate safeguards in place to protect the security of all the systems of records and PII systems for which it is responsible. Additionally, individuals that have privacy data contained in the agency's systems will not have knowledge that their personal information is included in a system of records and/or whether it is adequately protected.

An on-going effort is being made by the Privacy Advocate along with each Department's Assistant Executive Director to review the respective Department's systems of records and PII systems to determine whether the Department should have a PIA analysis done.

Recommendation: Privacy impact assessments should be performed for all new and existing system of records.

Auditee's Response to Recommendations

ITPP concurred in the recommendation and indicated that efforts were already underway to comply. No timeline was provided regarding when the recommended privacy impact assessments would be completed.

OIG's Comments on Auditee's Response to Recommendations:

NA

Finding #4: Inadequate physical security over documents containing Privacy Act protected data

The Privacy Act states that each agency must have in place an administrative and physical security system to prevent unauthorized release of personal records.

During the April 15, 2009 meeting with Directorate of Epidemiology data systems personnel, we conducted a "walk through" audit to determine if privacy data was "physically" secured. We observed two shredding containers (one silver and one blue) in use in Epidemiology. The shredding containers held documents that contained privacy act protected information. The contents of the containers were periodically removed by contractors who performed the actual "shredding" of documents. We observed that the silver container was locked but overflowing with documents. The overflow documents could be easily removed. This container was near the front entrance of Room 604. The other container was a large blue paper recycling bin with a roll-away top on it but no lock. This container was outside the office of the AED of Epidemiology, Room 604C. The facilities management chief stated that no one had contacted their office about emptying the locked container or securing the unlocked container.

After we contacted Facilities Management, the lock box was emptied and a lock was put on the blue bin with a slit carved in the roll away top for inserting documents.

Additionally, one program analyst that handled hard copies of CATI documents that contained PII, such as the names and addresses of patients from NEISS hospitals, did not store documents in a locked file cabinet. The analyst stated that the data was held for one week and then shredded.

While meeting with a Human Resources (EXRM) official, we noted that the file room where the staffing case files and employee relations files (both of which contain PII) were stored was left open during the day. CPSC employees have access to the EXRM office between 7 AM-5 PM and could easily walk into the file room and look around. The file room has a lock on the door and is locked at night. The employee relations files are kept in a safe in the file room. On the day of the meeting with EXRM, the safe was open. The EXRM official estimated there were 100 staffing case files and a similar number of employee relations files. The official did not have an inventory of the contents of the files.

While meeting with a Division of Information Management (ITIM) representative, we noted the boxes containing Freedom of Information Act (FOIA) documents were kept in an open file room during normal business hours. There were boxes of FOIA and privacy type data under a table that had a computer, printer and scanner on it in a hallway in the FOIA office. Additionally, several offices in ITIM contained opened boxes of unsecured FOIA records.

EXRM and ITIM officials felt that having an open file room and safe during normal business hours created minimal risk.

However, improperly secured privacy data, such as name, address, phone number and social security number (SSN), can be taken by any employee or contractor having access to the CPSC area in question and used for inappropriate or unauthorized purposes.

Recommendations: In order to more adequately secure the various offices examined, the following recommendations are provided:

1. Epidemiology management should check the shredding containers twice a month and, if boxes are full, request that the shredding service pick up and shred the contents of the containers;
2. Analysts who work on documents that contain Privacy Act protected data should be required to secure said data in a locked file cabinet at the end of the duty day;
3. Both EXRM and ITIM should restrict access to their offices at all times by having locked file rooms that can only be accessed by Directorate employees that have a need to have access to the files;
4. ITIM files should be stored in a file room, or be in some other way secured, when not in use, rather than in boxes in an unsecured area.

Auditee Responses to Recommendations:

EXRM stated that their file room is restricted space and only EXRM staff is authorized to have unescorted access in the file room area. Other CPSC employees and visitors to HR are greeted at the front desk. Also, they have posted a restricted area sign on the door. Additionally, the safe is locked when not in use.

ITIM stated that their file room in 502 is secured with a combination lock. The file room is left open only during office hours because of the constant use of the files and copier, which is in the room.

OIG's Comments on Auditee's Response to Recommendations:

At the time of the field work, no restricted area sign was posted on the door in EXRM nor was it apparent that anyone entering the file room would be stopped. We were not "greeted" at the front desk and did not see anyone seated near the file room to prevent unauthorized employees from gaining access.

At the time of the field work, the ITIM file room was open and anyone could access it particularly if they used the copier. Also records in file folders can be opened easily. Additionally there were open boxes containing documents in the hallway under a computer and scanner in the ITIM office. Finally, although the room is secured at night we found no indication that the doors are locked when the supervisor leaves the office on break or lunch.

Finding #5: Inadequate training of employees regarding their responsibilities under the privacy program

The agency is required to provide both general privacy awareness training to all employees and specific "duty related" training to certain employees related to their responsibilities under the privacy program. As detailed below, there is room for improvement in the way the agency meets both of these requirements.

The Privacy Act of 1974 requires agencies to follow certain procedures for collecting and safeguarding information in a system of records.

OMB Memorandum M-07-16 states that agencies should have already implemented the training of employees on their privacy and security responsibilities before providing access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

CPSC Directive 1435.1 states in relevant part that the privacy of an individual is a personal and fundamental right that shall be protected and respected. To that end, appropriate administrative, technical and physical safeguards shall be established, based

on the media (paper, electronic, etc.) involved, to ensure the security of records containing Privacy Act protected information and to prevent compromise or misuse of the records during storage or transfer.

CPSC Directive 1435.1 also states that the SAOP shall plan and conduct training, consistent with the requirements of the Privacy Act for commission employees and for those individuals having primary responsibility for implementing the commission's privacy program.

CPSC Directive 1435.1 requires that all system of records managers, as well as employees and contractors, who regularly work with records containing personal information, be instructed on the pertinent rules and requirements of the Privacy Act. The SAOP is responsible for ensuring that all employees and contractors who regularly work with records containing personal information receive training in the appropriate requirements of the Privacy Act, OMB Circular A-130, and CPSC Directive 1435.1. Training must adequately inform all employees of their responsibilities for handling or maintaining personal information.

Finally, CPSC Directive 1435.1 states that system managers are responsible for providing on-the-job training to the employees and contractors who utilize their systems. This training must be directly related to both the system of records in question and the specific Privacy Act requirements of the work performed by the individuals receiving the training.

The IG found that general privacy awareness training is provided annually to all CPSC employees as required by OMB Memorandum M-07-16, however, the training does not provide for a quiz after each section or a test at the end to measure the retention of the subject material. Currently, it is possible to receive credit for completing the training by clicking through the training screens without reading them. A test would add value to the process by ensuring that the employee had at least read the material, would aid in retention, and would help ensure that the training is achieving its stated goal of reducing the risk of a security breach.

Emails to remind employees and contractors to take the training were initially only sent out quarterly. In November and December they were sent out monthly. If the agency wants everyone to complete the training in the first quarter of 2009, they should send the e-mails out more frequently, perhaps bi-weekly.

Another approach would be to send out "privacy training refresher emails" periodically throughout the year to remind employees of their responsibilities regarding protecting Privacy Act protected records. When asked by the auditor why the agency did not do this, the Privacy Advocate stated they did not have time to dedicate to this effort.

The training process could also be improved through the adoption of certificates of completion. These certificates could be given out to personnel when they had finished taking training and they could serve as back-up documentation to the training completion list that EXIT maintains. The use of training certificates would also make it easier for

supervisors to track their employees training status, currently these supervisors have to request a copy of the training list that EXIT maintains to verify their employees training status.

The agency was not able to provide documentation that Office of Information and Technology Services (EXIT) staff had received the specialized training required by OMB Memorandum M-07-16. The ISSO sent the auditor an email from the Chief Information Officer requesting that EXIT staff take several networking security courses in the SkillSoft online training system before August 31, 2008 to respond to Federal Information Security Management Act (FISMA) requirements regarding this training. The ISSO stated that he could personally attest to the fact that all required staff completed at least one of the security courses by the specified due date. However, the agency was ultimately unable to provide any documentary proof that the training in question had been accomplished in FY 2008.

Both the SAOP and the Privacy Advocate stated they had not taken specialized privacy program training in two years due to the fact that they were not able to locate any suitable courses on managing a privacy program. For four of the five directorates and/or offices we surveyed, the required specialized privacy training had not taken place. These included: Epidemiology, the Division of Information Management, Human Resources and the Equal Employment Opportunity Office. The only directorate or office surveyed who had met this requirement was the Office of General Counsel (OGC) The OGC was able to meet this requirement by locating and attending specialized privacy training conducted by the American Society of Access Professionals.

There were 3 major causes of this finding. First, training certificates for taking the on-line general privacy training awareness course were not given out. This made it difficult to track who had or had not completed the training. According to the Privacy Advocate this was due to the lack of resources. The auditor found that it is possible to download a certificate template from Microsoft and use it as a certificate of completion. Second, evidence that specialized training for IT staff had taken place could not be provided due to lack of record keeping by management and a new training system, implemented at the time of the audit field work, which is incapable of uploading the old training records.

Finally, specialized privacy training in other directorates, besides IT, was not provided due to management's failure to hold on-the-job training for employees and assigned contractors in the specific requirements of a system of records related to their jobs.

The effect of privacy training not being given is that employees are not being informed of their specific responsibilities and obligations to safeguard Privacy Act protected information. The lack of training also results in employees not being aware of the potential consequences of a breach of security.

Recommendations: Privacy training efforts can be improved by:

1. Ensuring that all offices/directorates in the agency conduct and document specialized training for all their employees that handle PII that is “job specific” to their duties and position, as required by OMB Memo 07-16.
2. Issuing training certificates to employees that complete privacy training;
3. Requiring IT management to keep documentation of the completion of specialized training by themselves and their subordinates;
4. Utilizing quizzes and testing to aid in the retention of course material;

Auditee Responses to Recommendations:

EPDS stated that they planned to conduct specialized privacy training beginning in the first quarter of 2010.

ITPP stated that they are implementing the Global Learning training program for privacy and security for the Agency.

ITPP does not feel that it would be an effective use of their time to use certificates of completion for privacy awareness training and specialized privacy training.

OIG’s Comments on Auditee’s Response to Recommendations:

We feel that ITPP should develop and use training certificates to document the completion of the specialized privacy training.

Finding #6: Position descriptions of privacy program officials fail to reflect their duties related to privacy

The position descriptions of two key privacy officials do not adequately address their duties related to the privacy program. The Office of Personnel Management (OPM) website describes a position description in these terms, “. . . a statement of the major duties, responsibilities, and supervisory relationships of a position. In its simplest form, a PD indicates the work to be performed by the position. The purpose of a PD is to document the major duties and responsibilities of a position, not to spell out in detail every possible activity during the work day.”

The position description for the agency official designated as the Senior Agency Official for Privacy (SAOP), who is also the Division Director of ITPP, discusses the senior policy analyst functions of the position, such as being responsible for planning, organizing, staffing, coordinating and controlling the IT program and serving as the CIO for the CPSC. It does not include any of the privacy related duties for which she is

responsible. The position description does not include numerous privacy requirements discussed in CPSC Directive 1435.1, Policies and Procedures pursuant to the Privacy Act or CPSC Directive 1435.6, Privacy Impact Assessment Policy. These include:

Providing policy guidance for and coordinating and overseeing administration of the privacy program to ensure compliance with policies and procedures in the privacy act and OMB Circular A-130;

Updating and maintaining CPSC Directive 1435.1 and other guidance to ensure timely and uniform implementation of the privacy program; ensuring that the privacy program is periodically reviewed by the IG or other officials, having oversight responsibility for implementation of the privacy program;

Evaluating the ramifications for privacy of legislative, regulatory and other policy proposals and assessing the impact of technology on the privacy of personal information;

Providing the FISMA privacy material to the Office of Inspector General and submitting the Privacy Management Report (section D of FISMA report) to the CIO;

Planning and conducting training consistent with requirements of the Privacy Act for all employees; and

Having oversight responsibility for implementation of the Privacy Impact Assessment (PIA) program.

The position description for the privacy advocate does not cover any of the assigned privacy advocate duties, which as they were described to the auditor consist of:

Keeping track of employees' privacy awareness training and sending out reminders;

Conducting training on the PIA program for all commission employees that have responsibility for implementing the privacy program;

Directing the day to day activities of the PIA program;

Determining when and if a PIA is needed;

Ensuring that required PIAs are conducted.

The current SAOP was appointed in 2006 and the PD for her position has not been updated to reflect her duties related to the privacy program. Additionally, the Privacy Advocate's position description has not been updated to reflect her duties related to the privacy impact assessment process or coordinating the agency's privacy awareness training.

Recommendations: Update the position descriptions for the senior agency official for privacy and the privacy advocate to reflect their privacy program responsibilities.

Auditee Responses to Recommendations:

ITPP correctly notes that, technically, the duties in question are collateral duties and thus are not required to be included in the SAOP or Privacy Advocates position descriptions.

OIG's Comments on Auditee's Response to Recommendations:

Although the duties of the SAOP and Privacy Advocate are "technically" collateral, they are also sufficiently important that OMB required the agency to report whom was holding the positions. Based on the time they require and their importance we believe these duties should be included in the position descriptions of the individuals who hold them.

Attachments to Report

Attachment 1

EXIT Comments

Date: November 3, 2009

TO : Christopher Dentel, Inspector General, OIG

THROUGH: Patrick Weddle, Assistant Executive Director, EXIT

FROM : Mary Kelsey, Director, ITPP

SUBJECT : Office of the Inspector General Review of CPSC Privacy Program, October 2009

There are several recommendations in subject report we would like to respond to.

1. IG Recommendation: Ensure contractor compliance with physical security of personal computers (pcs) and privacy data requirements by auditing physical security of notebook computers at hospital facilities, installing encryption and security software package, and considering using tracking devices on the CPSC pcs used at the hospitals.

ITPP Response: All contractor computers are configured to include encryption and security software. Tracking devices do not seem practical or cost effective. Since the data is encrypted and protected, in the event of loss of a computer, the data would be secure.

2. IG Recommendation: Improve privacy training efforts by including quizzes for knowledge retention of material, implement training certificates for employees that complete privacy training, require management to retain documentation on completion of specialized training by themselves and their employees and require each office to conduct specialized privacy training for employees that handle privacy information that is relevant to the type of work that they perform.

ITPP Response: For FY 2010, we have moved to Global Learning training programs for privacy and security training. The new IT security training has been implemented. We are expecting the Privacy Training to be implemented in the first quarter of 2010. These programs have the capability for tracking employee completion of training. In 2009, employee completion of training was tracked using email confirmation from the employee or online tracking using Sharepoint. Each office is currently required to conduct specialized privacy training for employees that handle privacy information as described in CPSC Directive 1435.1 19(b). As far as network security training and privacy training, printing and distributing certificates of completion did not seem practical or the best use of the Information Security Systems Officer or the Privacy Official's time.

3. IG Recommendation: Consider rewriting position description for the Senior Agency Official for Privacy and the Privacy Advocate.

ITPP Response: Because this is a collateral duty, it is not specifically described in the position descriptions. The Privacy Advocate's duties are noted in the annual performance elements and can be added to the Senior Agency Official for Privacy's performance elements.

4. IG Recommendation: Implement procedures to check the shredding containers that contain privacy identity information documents bi-weekly, secure privacy data being analyzed in a locked cabinet, and restrict access through the use of combination locks or keys to file rooms that contain privacy information.

ITPP Response: Each individual office is responsible for checking the status of shredding containers that contain privacy identity information and keeping cabinets locked. ITPP has a vendor that cleans out the shredding containers once a month. If more frequent pick up is needed, it is incumbent on the office to make a request. Shredding containers come with locking devices and ITPP can notify the vendor and request replacement containers with new locks whenever needed by an individual office.

5. IG Recommendation: Establish redaction of privacy identification information on injury investigation report attachments that are scanned into the CPSC net.

ITPP Response: We have identified a technical solution and are in the process of implementation.

6. IG Recommendation: Ensure security of all system of records containing privacy identification information by conducting privacy impact assessment reports.

ITPP Response: Efforts are currently underway to conduct Privacy Impact Assessments for all established System of Records, whether electronic or paper systems. PIAs will be posted to cpsc.gov once they are completed.

Attachment 2

EPDS Comments

Date: November 4, 2009

TO : Christopher Dentel, Inspector General, IG
THROUGH: Russell Roegner, Associate Executive Director, EP
Thomas Schroeder, Director, EPDS
FROM : Cathleen Irish, Chief, EPDSC
SUBJECT : Comments on the October 2009 Review of CPSC Privacy Program draft report

Thank you for the opportunity to comment on the draft report – it is my understanding that these comments will be included in your final report. As you know, I had some questions about what sort of comments were expected. My confusion arose from the fact that I was the only person in EPDS who was asked to provide comments, despite there being several people who participated in the information gathering stage, including another EPDS Branch Chief and the Division Director. Since EPDS was accidentally omitted from the invite list for the exit conference, I also did not have the opportunity to hear whatever instructions might have been provided then. I suggest for future reports, that you provide together with the draft some general information on what the next steps will be and what sort of comments you are looking for (corrections to facts, comments on suggested remedies, etc.). It would be very helpful to those of us who are new to this process.

Comments on each of the report findings relevant to EPDS are provided below. They were prepared in consultation with the Director of EPDS and the AED for Epidemiology.

Finding #1 – Physical Security and Encryption of Laptops used by Contractors working on the NEISS Program

- On page 7 of the report it says, “A coder enters injury data from hospital forms and may conduct a follow-up investigation...” NEISS coders do not conduct follow-up investigations. Rather, when a NEISS case is selected for follow-up, the hospital coder is prompted to provide contact information for the patient. In some hospitals the NEISS coders may contact the patient to request permission to provide their name to CPSC, but the investigations are assigned either to CPSC field staff or to one of two companies currently under contract to CPSC to do follow-up interviews by telephone.
- As of this writing, over 80% of the NEISS laptop computers in use by hospital coders have been switched over to the new communications program. Each of these laptop computers also has hard disk encryption, anti-virus software, and patch management. We hope to have the remaining laptop computers switched over by the end of the year.
- On page 7 when discussing the two laptop computers that were stolen on 12/31/2005 and 2/27/2008, it is not clear that EPDS did report the theft of the equipment through the appropriate channels at CPSC and that we reported the

2/27/2008 incident to the ISSO. In each case both the Report of Property for Survey and the Physical Security Offense/Incident Reports were submitted. Copies of these documents are attached. What we failed to do in the earliest incident was report it to the ISSO as a possible PII incident, but as a result of that earlier incident we were informed that should a similar incident occur in the future we should report it to the ISSO. When the 2/27/2008 incident occurred we reported it by phone to the ISSO. We researched what information was on the laptop computer that was stolen and provided that to the ISSO as well. We do not believe that there was any PII on the laptop computer at the time it was stolen. That hospital does not provide date of birth and there were no open requests for victim ID at the time the laptop computer was stolen. Patient ID provided in response to earlier requests would have been deleted before the laptop computer was stolen.

- On page 8 of the report it says, "...since the NEISS laptop computers were not handling privacy information." The statement actually is referring to the equipment used by the CATI contractors, so the sentence should read, "...since the CATI laptop computers were not handling privacy information." NEISS laptop computers do contain PII and we are in the process of replacing them with laptop computers having hard disk encryption.

The report recommends five steps to address the issues of physical security and data encryption on the NEISS and CATI laptop computers:

1. Initiate procedures for securing laptops that contain NEISS data at hospitals, contractor residences and vehicles.

We have provided locks to the NEISS coders and asked that they use them. After the theft of a NEISS laptop computer from a coder's vehicle, we sent a message to all NEISS coders stating that the laptop computers should not be left unattended in a vehicle. We will follow-up with a memo to the coders reminding them of their responsibility to secure the NEISS laptop computer at all times. However, we do not believe it is necessary for the coders to use the lock at home. Most homes do not have furniture to which a computer could be secured.

2. Install encryption and security software on all laptop computers at NEISS hospitals and CATI contractor offices.

Over 80% of NEISS laptop computers now have encrypted hard disks and security software. The remainder should have it by the end of the year. We will request that EXIT issue new equipment to the CATI contractors with hard disk encryption and security software as soon as possible. We will provide locks to the CATI contractors and require that they use them.

3. Audit physical security of laptops at hospital facilities to ensure procedures are followed.

We will ask analysts and contractors conducting evaluation site visits to check that the NEISS laptop computer is properly secured and to include their findings in their report.

4. Ensure contractor compliance with physical security of laptop computer and privacy data requirements is mandated in the statement of work for NEISS hospital contracts.

The hospital and third party coder contracts already contain standard language regarding the contractor's obligation not to disclose information and to protect it as required by the Privacy Act. We will work with the Contracts office to add language to NEISS contracts which states that the contractor must ensure the physical security of the laptop computer by using the lock provided.

5. Consider using tracking devices on the personal computers used the hospitals.

We will defer to EXIT on this question – they are now configuring and maintaining the equipment used by NEISS coders.

Finding #2 – Privacy Awareness Training

We plan to conduct specialized privacy awareness training in EPDS annually beginning in the first quarter of FY 2010. In addition, new employees will complete the specialized training within the first 30 days on the job. In addition, the AED for Epidemiology has directed all supervisors to add a requirement to each performance plan that employees handle PII in accordance with CPSC policy.

Finding #4 – Physical Security of Privacy Documents

1. Epidemiology management should check the shredding containers twice a month and if boxes are full request that the shredding service pick up and shred the contents of the container.

As users of the shredder bins, EP management checks the containers much more often than twice a month. On the occasion cited in the report, the replacement bin had recently been delivered (within the past day or so) and the absence of the lock had not yet been noted. On several earlier occasions I had contacted the help desk or spoken with someone in Facilities Management when they replaced the shredder bin with an unlocked bin (see attached help desk ticket). We have asked EPDS staff to also be sensitive to the status of the shredder bins: to refrain from overloading them and to request that they be emptied when they are full.

2. Analysts who work on documents that contain privacy data should be required to secure data in a locked file cabinet at the end of the day.

Over the last few months we have implemented a number of changes to ensure that documents that are being processed within EPDS are secured when not in use, but we still have a ways to go on this issue. Through the specialized privacy and security awareness training planned for the first quarter of FY 2010 and new standard operating procedures for EPDS we will make all EPDS staff aware of their responsibility to properly secure documents containing personally identifiable information.

Finding #5 – Epidemiologic Report investigations having PII data attachments

- The 1/15/2009 email sent by the EPDS Data Operations Branch Chief is not characterized correctly in the report. The email asked that analysts redact social security numbers from death certificates. These are the death certificates that we purchase from the states and that go into DTHS or ADBT. At that time we had not yet realized social security numbers were also showing up in IPII documents and IDI attachments. Sometime after the initial request, we recognized that MECAP reports submitted for IPII also could contain social security numbers and that people weren't remembering to check death certificates for social security numbers. We then modified the coversheet used for death certificates to require each person handling them while they were being processed in EPDS to affirm that all social security numbers had been removed from the documents. We also began requiring that a similar coversheet be affixed to MECAP reports.
- The report suggests that EPDS should be removing all personally identifiable data from IDIs, but that is incorrect. It is true that we have no need of social security numbers and we agree that they should be removed. However, other information such as name and address has value to CPSC staff using these reports. We have always retained that information in our files and would argue that we should continue to do so. This type of data enables us to recognize related reports and also allows us to recontact the victim should that become necessary at a later date.

1. Staff should delete privacy data before scanning investigation reports and attachments into the website. Additionally staff should delete privacy information from old records.

We will make every effort to remove social security numbers from incoming documents. We have asked that the Division of Field Investigations redact social security numbers from IDI reports before they are written to the CPSC network. EPDS staff will review incoming reports to verify that attachments do not include any social security numbers and when a social security number is found in an IDI report, the field investigator and supervisor will be reminded of the requirement to redact this information. We will explore options and seek funding for removing social security numbers from documents that are already in the system. In the meantime, when we notice or are made aware of the presence of a social security number in a document, we will redact it. Please note that most social security numbers in CPSC data are for deceased individuals and while there is some risk of identity theft early on, that risk diminishes over time.

Attachments

Attachment 3

EXRM Comments

From: Schwab, Beth
Sent: Thursday, October 29, 2009 9:06 AM
To: Rosenbusch, Lynne
Subject: FW: Privacy Report and Exit Conference Slides

I have concern with a statement in the draft report –

1. Finding #3 on page 12...Outdated PDs cannot be used to set annual goals and objectives with regards to the privacy program. This statement is inaccurate. The PD is a statement of the major duties, responsibilities, and supervisory relationships of a position. Annual goals and objectives should not be derived from the PD. A goal could be reflected in a performance plan.
2. Finding #4 on page 12 & 13... HR file room is left open – this is restricted space, only the HR staff is authorized to have unescorted access in the file room area. Other CPSC employees and visitors to HR are greeted at the front desk. We are not in the practice of allowing CPSC employees or visitors to move around EXRM space. To establish a clear boundary for CPSC employees and visitors, we have posted a restricted area sign on the door. Additionally, the safe is locked when not in use.

Thanks
Beth

From: Rosenbusch, Lynne
Sent: Monday, October 05, 2009 7:28 AM
To: Dentel, Christopher; Schwab, Beth; Cheung, Julie; Manley, Patrick; Glatz, Linda; Kelsey, Mary; Irish, Cathleen
Subject: Privacy Report and Exit Conference Slides

Attached is the privacy report draft and exit conference slides.

If you have comments please email me so I can incorporate them into the final report.

<< File: Draft Report Sept 17.doc >> << File: exit conf.ppt >>

Lynne Rosenbusch
Auditor
CPSC/OIG
lrosenbusch@cpsc.gov
301-504-7681

Attachment 4

ITIM Comments



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST—WEST HIGHWAY
BETHESDA, MD 20818

Memorandum

DATE: October 20, 2009

TO: Christopher, Dentel, Office of the Inspector General

FROM: Todd A. Stevenson, *Todd Stevenson* Director, Division of Information Management ("DIM")
and Office of the Secretary ("OS")

SUBJECT: Comments Regarding the Draft Report: Review of CPSC Privacy Program,
October 2009

This regards the parts of the draft report that discuss the DIM/OS physical security, the open file room and documents unsecured in the offices. Our file room in Room 502 is a secured file room with a combination lock and contains the Official Records of the Commission maintained by OS and the Freedom of Information Act ("FOIA") processed records. The file room is left open only during office hours, because of the constant use of the files and the copier, which is in the room. Only agency personnel with a need to use the room or the files are allowed in the file room. Records that may contain personal records are not left in the open and are secured in file folders, generally filed by the name of the manufacturer involved. The file room is locked at the end of the business day.

Regarding the records open to the supervisors' offices, the records are generally from processed FOIA files and are being actively processed in response to FOIA requests. Any records containing privacy information are maintained in closed folders and boxes. At the end of the business day, we close and lock the supervisors' offices and the front door to the entire suite.