



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

CHAIRMAN INEZ M. TENENBAUM

November 18, 2009

The Honorable Peter Orszag
Director
Office of Management and Budget
725 – 17th Street, NW
Washington, DC 20503

Dear Director Orszag:

As required by the Office of Management and Budget, the U.S. Consumer Product Safety Commission (CPSC) is submitting the Office of Inspector General's Federal Information Security Management Act (FISMA) 2009 report.

I have reviewed the FISMA report and agree with the Inspector General's assessment. Our plan to remediate any outstanding issues will be reflected in our quarterly Plan of Action and Milestones.

Information technology security and privacy compliance are critical to the Commission's mission to protect the public from unreasonable risks of serious injury or death from consumer products under the agency's jurisdiction. CPSC will continue to conscientiously manage these areas to ensure our success.

Very truly yours,

A handwritten signature in black ink, appearing to read "Inez M. Tenenbaum".

Inez M. Tenenbaum

Enclosure

U.S. CONSUMER PRODUCT SAFETY COMMISSION



OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT

REPORT

October 30, 2009

Federal Information Security Management Act Report
Table of Contents

	Page
EXECUTIVE SUMMARY	i
Office of the Inspector General's Results	
INTRODUCTION	1
Background	1
Objective	2
Scope and Methodology	2
RESULTS OF EVALUATION	2
Prior Findings, Recommendations, and Actions Taken	
Security Management Controls	3
Security Operation Controls	5
Security Technical Controls	6
Performance Measures	8
Privacy Program and Privacy Impact Assessment Processes	9

Office of the Inspector General
U.S. Consumer Product Safety Commission
Washington, D.C. 20207

FEDERAL INFORMATION MANAGEMENT ACT REPORT

EXECUTIVE SUMMARY

Office of the Inspector General's Results

To meet the requirements of the Government Information Security Reform Act (GISRA), and its successor, the Federal Information Security Management Act (FISMA), the Consumer Product Safety Commission's (CPSC) Office of the Inspector General (IG) contracted with Grant Thornton, LLP to perform an independent audit of CPSC's automated information security control procedures and practices in Fiscal Year 2001. The audit included tests of entity-wide controls and six of CPSC's 49 application systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology Special Publication (SP) 800-XX, Draft Self-Assessment Guide for Information Technology Systems, March 9, 2001 to test security controls. The results of the Audit of Automated Information System Security, August 16, 2001, and the annual follow-ups to it, in conjunction with the independent reviews required by FISMA and audits with privacy (Review of the CPSC Privacy Program) or information technology aspects (CFO Act Audit, etc.), served as the basis for the IG's Fiscal Year 2009 evaluation.

This year's FISMA evaluation found that although much work has been done and the CPSC's IT system had retained its certification and accreditation, much work remains to be done. For example, the CPSC's Security Plan of Action and Milestones (POAM) can, and should, be better integrated into the agency's planning and management processes. The IT challenges facing the agency are particularly relevant at the present time as the agency deals with both the implementation of the Consumer Product Safety Improvement Act (CPSIA) in general and with the CPSIA's specific impacts on the agency's IT operations.¹

Although the CPSC has continued to develop its privacy program in an effort to meet the non-IT information security standards tested by FISMA and set out in a variety of OMB and related requirements, including those relating to the Privacy Act and the protection of personally identifiable information (PII), there is still room for improvement. Although much work has been done in drafting and beginning the process of implementing privacy and information security policies, not enough has been done to implement and test compliance with these policies.

¹ The CPSIA requires the development of a database of publicly available information on incidents involving injury or death required under section 6A of the Consumer Product Safety Act and the integration of the database into the Commission's overall information technology improvement objectives and plans.

Office of the Inspector General
U.S. Consumer Product Safety Commission
Washington D.C. 20207

FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

INTRODUCTION

Background: On October 30, 2000, the President signed into law the Fiscal Year (FY) 2001 National Defense Authorization Act, which included Title X, Subtitle G, the Government Information Security Reform Act (GISRA). On December 17, 2002, GISRA was superseded when the President signed into law the Electronic Government Act. Title III of this Act, the Federal Information Security Management Act (FISMA) along with OMB policy, lays out a framework for annual IT security reviews, reporting and remediation planning. FISMA seeks to ensure proper management and security for information resources supporting Federal operations and assets. The Act requires Inspectors General to perform an annual independent evaluation of their agencies' information systems security programs and practices.

To establish a baseline to help it meet the requirements outlined above, the CPSC's Office of the Inspector General (OIG) contracted with Grant Thornton to perform an independent audit of CPSC's automated information security control procedures and practices in FY 2001. The requirements of the audit included:

- Evaluating and testing the internal controls, evaluating weaknesses and identifying the degree of risk for the related weakness.
- Testing the effectiveness of the information security controls on a sample of CPSC's systems.
- Assessing whether CPSC's information security policy, procedures, and practices comply with Federal laws, regulations, and policies.
- Recommending improvements, where necessary, in security record keeping, internal security controls, and system security.
- Identifying the degree of risk associated with identified internal security controls weaknesses.

The audit included tests of entity-wide controls and six of CPSC's 49 applications systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology Special Publication (SP) 800-XX, Draft Self-Assessment Guide for information Technology Systems, March 9, 2001 to test security controls. The objective of the audit was to determine whether CPSC's automated information system was adequately safeguarded.

In its report, Audit of Automated Information System Security, Grant Thornton, identified material weaknesses in CPSC's management, operational, and technical controls policies, procedures, and practices. According to the report, the conditions of these controls could permit the modification or destruction of data, disclosure of sensitive information, or denial of services

to the users who require the information to support the mission of the CPSC. In addition, it was reported that the CPSC did not have a capital budget for IT security. Without appropriate capital budget planning, Grant Thornton was concerned that CPSC's management might not be able to properly implement and maintain resources to ensure system safeguards.

Objective: In compliance with FISMA, to perform an annual independent evaluation of the information security program and practices of the agency in order to determine the effectiveness of such program and practices.

Scope and Methodology: The evaluation was conducted from August to October of 2009. This evaluation consisted of: an evaluation of a representative sampling of all types of agency systems, a review of agency progress in implementing and managing the Plan of Action and Milestones (POA&M) process, and an assessment of the agency's certification and accreditation process. In addition, work previously performed as part of the Chief Financial Officer's Act Audit and the Review of the CPSC Privacy Program was also relied upon.

This review constitutes both a follow-up of the findings and recommendations resulting from earlier audits and a review of the CPSC's implementation of recent IT and Personally Identifiable Information (PII) security criteria. Emphasis was placed on the weaknesses that had been previously identified in the CPSC's management, operational, and technical controls and the actions taken to resolve these weaknesses. Additionally, special attention was placed on the certification process, CPSC's Information System Security Plan, and the Plan of Action and Milestones, as well as the status of implementation of each.

The status of each of these items was reviewed and discussed with the Chief Information Officer, Senior Agency Official for Privacy, their staffs, and the Information Security Officer. The Budget Officer provided budgetary information. Documentation developed by both CPSC officials and contractor personnel was reviewed as necessary.

RESULTS OF EVALUATION

Prior Findings, Recommendations and Actions Taken: The FY 2001 audit of CPSC's information security program revealed several material weaknesses in CPSC's security policies, procedures, and practices. Specifically, CPSC management had not implemented sufficient management, operational, and technical controls. All previously identified material weaknesses have now been corrected. No additional material weaknesses have been identified. However, due to a combination of budget limitations and the new security system requirements promulgated by NIST and OMB, the CPSC failed to accomplish all of the new security requirements by their implementation target dates. All recommendations are considered open until all of the underlying weaknesses have been corrected. A summary of Prior Findings, Recommendations, and Actions Taken follows:

1. Security Management Controls

Prior Finding: Security management controls are enterprise-wide procedures for managing and assessing the risks and security controls of a system over its life cycle. Because CPSC management had not implemented sufficient management controls in the areas of risk management, review of security controls, life cycle management, authorized processing, and system security planning, the techniques and concerns that are normally addressed by management were not fully implemented. OMB Circular A-130, Appendix III requires sufficient management controls in these areas. This condition appears to have been due to CPSC management not having the resources necessary to make the implementation of Security Management controls a priority.

Prior Recommendation: CPSC management should implement sufficient management controls in the areas of risk management, review of security controls, life cycle management, authorized processing, and system planning in order to ensure efficient and effective management of the IT systems and its inherent risk.

Actions Taken: CPSC contracted with Patriot Technologies (Patriot) to develop an Information System Security Plan (ISSP), January 31, 2002, that conforms to OMB Circular A-130 requirements and responds to Grant Thornton's findings. The new ISSP provides CPSC with an overall security plan describing a functional information systems security framework. It describes CPSC organizational responsibilities for information system security.

In FY 03, CPSC contracted with PEC Solutions Inc. (PEC) to perform systems certification and accreditation and to develop a plan to ensure adequate management control in the areas of risk management, review of security controls, life cycle management, authorized processing, and system planning. In addition to the ISSP, a System Development Life Cycle (SDLC) Plan and Business Continuity Plan were prepared. PEC successfully completed the work contracted for regarding system certification and accreditation, risk management, and the development of a SDLC Plan and a Business Continuity Plan. All previously identified "material weaknesses" in these areas were addressed. Although PEC did not find that "full" certification and accreditation of CPSC's systems was appropriate in FY 03, they did issue an "interim approval" and indicated that full certification would be appropriate once certain recommendations set out in their report were achieved.

In FY 04, after those deficiencies that were found to be "material weaknesses" were addressed, the CPSC began the process of implementing the recommendation set out in these plans to deal with less serious security deficiencies ("high" priority security vulnerabilities). Ten of the eleven "high" priority security vulnerabilities were mitigated. The eleventh, after a new cost risk analysis was completed, was reclassified as an "acceptable risk." As a result of the work done in FY 04, the interim label was removed from the CPSC's system certification and accreditation.

In FY 05, in accordance with new OMB guidance, the CPSC began using NIST SP 800-26 to perform agency security self-assessments and began implementing new system configuration policies. Efforts continue to this day at to bring the CPSC into full compliance with all other FISMA and OMB requirements.

In FY 06, new security system requirements previously promulgated by NIST and OMB became mandatory. In order to retain accreditation and certification of their computer system the CPSC was required to have their security controls independently tested and evaluated annually. Due to funding limitations this was not done in FY 06.

In order to both meet the accreditation and certifications requirements outlined above and to determine whether the security controls identified for the CPSC Network General Support System in the System Security Plan were implemented correctly and effectively, in FY 07 the Office of Inspector General conducted a Security Test and Evaluation (STE Evaluation) in accordance with NIST SP 800-53. The STE Evaluation identified sixty-three (63) vulnerabilities for the CPSC Network General Support System. Of these, six were found to be high risk vulnerabilities, 31 were found to be medium risk vulnerabilities, and 26 were found to be low risk vulnerabilities. The STE Evaluation Report included a planned mitigation with an associated due date for each vulnerability identified.

In FY 08, the CPSC regained system certification. This was accomplished after the mitigation of the six high risk vulnerabilities found in the STE Evaluation and the successful approval and testing of the CPSC's IT Contingency Plan.

In FY 09, a fundamental problem with the CPSC's Plan of Action and Milestones (POAM) was found. OMB has determined that agency POA&Ms must reflect known security weaknesses within an agency and, ". . . shall be used by the agency, major components and program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps." Although recent changes have been made to help the agency address this shortcoming, the POAM has not historically been used by the CPSC as an affirmative management tool in addressing security weaknesses. Although it has historically done a good job of documenting known security weaknesses and prioritizing them, the agency has not used the POAM to either track or project the resources required or milestones necessary to address these weaknesses (as required by OMB). As a result, the agency lacks historical data regarding its past efforts and fails to take advantage of a powerful planning tool in addressing current and future IT security challenges.

Our review determined that the CPSC IT System had maintained its certification and accreditation and that the system's security controls were, in the opinion of management, tested and reviewed in so far as the agency continuously monitored the system. However, the Contingency Plan had, again, not been tested within the past year and no STE Evaluation or other formal review of security controls has been accomplished since FY 07. Although neither of these issues is sufficient to cause the CPSC to lose its system accreditation, they are both troubling.

The CPSC ISSP states that the security program shall provide for a review of the technical security control at least once every 3 years. OMB Circular A-130, Appendix 3 (section A.3. 3) states that security controls should be reviewed in each system when significant modifications are made to the system but at least every 3 years. The risk assessment currently being relied upon was completed in 2006 and is or will shortly be over three years old.

The CPSC has not begun the process of reassessing security controls over its IT system, possibly because of the impending major changes to the system required by the implementation of the Consumer Product Safety Improvement Act.

Because no review has been documented, the agency cannot show that existing security risks and vulnerabilities have been remedied and/or what new security risks and vulnerabilities exist. The CPSC should perform and document a formal review of its technical security controls on a regular basis.

2. Security Operational Controls

Prior Finding: Security operational controls are used to assess the security of the system processes and the people who interact with or operate those systems. Because CPSC management had not implemented sufficient operational controls in the area of personnel security, data integrity, and documentation, CPSC management was not able to address security procedures to focus on security mechanisms that affect the daily operation of the Commission. OMB Circular A-130, Appendix III requires that sufficient operational controls for personal security, data integrity, and documentation be in place. This condition may have been due to CPSC management not having the resources necessary to make implementation of operational controls a priority. The level of risk was rated “high” for personnel security and data integrity.

Prior Recommendation: CPSC Management should implement sufficient operational controls in the area of personnel security, data integrity, and documentation in order to ensure efficient and effective management of the IT systems in support of CPSC’s mission.

Action Taken: CPSC contracted with Patriot to develop the Information System Security Plan (ISSP). Patriot reported that in order for CPSC to adequately implement and maintain the requirements of the ISSP, a staff of three full-time personnel (information system security officer, network security engineer, and applications security engineer) would be needed. Qualifications for and responsibilities of each position were delineated in the ISSP.

Due to staffing constraints, CPSC recruited one of the three recommended positions (Information Security Officer) and contracted out the remaining responsibilities on an “as needed” basis. A contract was awarded to PEC Solutions Inc. (PEC) to produce a new ISSP that conforms with the resource constraints in place at the CPSC and sets out the specific steps (in the form of recommendations) necessary to implement the plan. The ISSP was completed just before the end of FY 03. Implementation of the recommendations contained in the ISSP, augmented by new requirement created by subsequent regulations, continued for the next several years. After several years of steady progress a lack of a security operational controls played a

role in the CPSC's loss of system certification in FY 07. In FY 08, certification and accreditation was regained when the needed security operational control was implemented.

The FY 09 FISMA review found that operational controls in the area of documentation remained problematic. In a number of areas the agency is meeting Federal guidelines in terms of the work being performed, but failing to adequately document what it is doing. For example, although much work has been done to attain and maintain system certification and accreditation at the CPSC, the agency has not documented its policy for establishing a certification and accreditation process that follows the NIST framework (as it is required to do).

In FY 2007, OMB mandated that agencies adopt security configurations for Windows XP and VISTA, as well as a policy for ensuring new acquisitions include common security configurations. (See OMB Memorandum M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," and OMB Memorandum M-07-18 "Ensuring New Acquisitions Include Common Security Configurations,") However, despite the fact that the FISMA Act (at section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them, there is no formal agency wide system configuration policy at the CPSC. There is also no formal agency policy implementing the procurement policies regarding desktop core configuration, required by FAR 2007-004. These procurement policies were designed to ensure that newly acquired IT equipment complies with the above referenced configuration requirements.

The theory behind the requirement for agency wide security configuration policies is that common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity and availability of Government information.

Although it appears possible that the agency may in fact comply with NIST common security configurations on an "ad hoc" basis, a formal policy regarding system configuration requirements should be adopted and implemented. This policy should include language ensuring that the correct requirements regarding system configuration are included in the appropriate IT acquisitions.

Currently, 78.7 percent of total CPSC staff and contractors with access to the CPSC system have completed security training. There is an additional "specialized" security training requirement for employees with significant IT security responsibilities; to date 92% of these employees have received the required training. The security training process could be improved in several ways. Training on the CPSC's policy regarding peer-to-peer file sharing should be added and the use of certificates of completion or some other means of documenting individual employees' completion of the training should be adopted.

3. Security Technical Controls

Prior Finding: Security technical controls are specific to the system's ability to identify, track, and act on authorized or unauthorized usage. Because CPSC management had not implemented sufficient technical controls in the areas of identification and authentication, logical access, and audit trails, CPSC management had left sensitive information vulnerable. This condition appears to have been due to CPSC management not having the resources necessary to make implementation of sufficient technical controls a priority. The level of risk was rated high for identification and authentication, and logical access.

Prior Recommendation: CPSC management should implement sufficient technical controls in the areas of identification and authentication, logical access, and audit trail in order to protect the information that is used to support the mission of the Commission.

Action Taken: The effectiveness of six of CPSC's systems and the underlying elements of each were tested during the FY 2001 audit. Weaknesses identified in controls related to these systems contributed to the overall condition of CPSC's information security program. Management was advised of specific weaknesses and recommendations, each of which was to be addressed during the implementation of the ISSP and Systems Certification and Accreditation contract. Weaknesses outlined in the ISSP were to be corrected in all applications. Additional systems were not tested because management was in the process of implementing prior recommendations, the implementation of which would alter the policies and procedures applicable to all applications. As reported in the management response to the original audit, CPSC requested funding in Fiscal years 1999 through 2002 without success to establish a capital budget for information technology. The need for such funds was also included, unsuccessfully, in CPSC's FY 03 and 04 budget requests. Budget requests cited the need for new investments to protect the current operating capability and efficiency of information technology. According to the Budget Officer, in the absence of a capital budget for information technology, CPSC has applied some savings from operating funds to this area. In FY 02, CPSC committed over \$500,000 from one-time salary savings to this area to develop an ISSP, address data system weaknesses, enhanced firewall intrusion detection capabilities, and other operating and system application enhancements. In FY 03, CPSC committed \$714,891 to this area in the form of salaries and other expenses. In FY 04, CPSC committed \$715,000 for its Information Technology programs. In FY 05, this figure rose to \$1,035,100. In FY 06, the CPSC spent \$2,082,050 on its IT programs. In FY 07, the CPSC committed \$6,300,000 to its IT program. In FY 08, the CPSC's commitment rose to 30 FTEs and \$13,000,000. Work on implementing the recommendations contained in the ISSP and more recent guidance continues.

In some cases the implementation of security controls has outstripped the documentation or generation of policies regarding same. In other cases, where the agency has developed policies, it has failed to provide agency wide training detailing them to its workforce. For example, the CPSC currently conducts continuous intrusion detection monitoring and performs an annual vulnerability assessment, but neither of these efforts are formally documented or covered by existing policies.

On the other hand, the agency has a policy prohibiting its employees from using peer-to-peer file sharing on Government computers, but does not explain this policy in its information security awareness, ethics, or any other agency wide training.

The CPSC's most recent Plan of Action and Milestones (POAM) report to OMB reflects the improvements that the CPSC has made as well as the work remaining before it. The agency has now resolved all material weaknesses as well as the "high" security vulnerabilities found by Grant Thornton and the 2007 STE Evaluation. However, it has failed to address all of the lower priority vulnerabilities found by these evaluations or to keep up with some of the more recent security requirements. The CPSC has failed to adequately address approximately thirty-nine (39) identified weaknesses, one of which is rated as a "high" security vulnerability and sixteen (16) of which are rated as medium security vulnerabilities.

The CPSC acknowledges its need for continued improvement. Over the past few years, the CPSC has met the following goals in its effort to improve its security technical controls: implementing a security awareness training program, providing a redundant cooling capability to the Agency's existing computer room air conditioning unit, providing the ability to quickly recover from an e-mail server failure by periodically taking and storing e-mail "snapshots" of the e-mail database, implementing the ability to perform automated system auditing, and implementing the monitoring of Internet usage.

Although they are properly reflected in the POAM, a large number of known weaknesses, one of them listed as a "high" priority, have still not been remedied. Perhaps more troubling, no firm plan for how to address them or scheduled completion dates have been established for them. For example, client sessions are not automatically terminated after a specified period of inactivity and the agency does not enforce explicit rules governing the installation of software by users; both of which it is required to do. A random audit of user workstations found multiple instances of user workstations with installed software for which there was no corresponding installation approval documentation.

Performance Measures: Security responsibilities and authorities have been defined for the Chief Information Officer, Information Security Officer, and program officials in CPSC's ISSP. The performance measures detailed in NIST 800-26 have been incorporated into existing organizational goals for IT security in the ISSP.

After the STE Evaluation in FY 07 resulted in the decertification of the CPSC's system, much work was put into regaining system certification, which was achieved in FY 08. NIST 800-53 controls were incorporated by the agency and future certification and accreditation work should have been consistent with the most recent NIST Special Publication requirements. It was assumed at this time that the remaining security vulnerabilities would be addressed as expeditiously as possible. However, in FY 09, it was found that only 5 of the existing 63 vulnerabilities shown in the 2007 STE Evaluation had been addressed and that no comprehensive testing and evaluation of the security of the system had taken place since 2007. The CPSC should conduct another STE Evaluation of its IT System.

4. Agency Privacy Program and Privacy Impact Assessment (PIA) Processes

Background: Historically, the Federal government has placed a much greater emphasis on IT security than on privacy or protection of personally identifiable information. The challenge facing the CPSC regarding protection of personally identifiable information and other sensitive data is in many ways even more pronounced than the challenge of information technology security. Although many of the challenges facing the agency regarding information system security can be addressed through technical improvements, the issues regarding personally identifiable information are more complex and will require the adoption of new policies, methodologies, and in many cases mindsets in the management of the agency. This area in particular has been subject to numerous new statutory and regulatory requirements in the past few years including recent guidance calling for the implementation of plans to eliminate the unnecessary use of Social Security Numbers and the review and reduction of the agency's holdings of personally identifiable information.

Status: The agency has made progress in privacy management in the past three years. In that time, a Privacy Impact Assessment process has been implemented and begun to operate, staff have been assigned to work in this area (previously this was treated strictly as an additional duty), and efforts have been made to draft and implement agency policies regarding training and the implementation of internal controls to ensure the protection of PII. However, as documented in a recent IG Audit, much work remains to be done in this area.

For example, the Senior Agency Official (SAOP) for Privacy and the Privacy Advocate (the two officials with the most responsibility for the Privacy Program) both have position descriptions that do not accurately reflect their duties. The SAOP's position description does not include numerous privacy requirements detailed in various agency directives and the Privacy Advocate's position description does not cover any of the assigned privacy program duties.

Additionally, although a Privacy Impact Assessment (PIA) program has been implemented by the agency, the program currently only results in the conduct of PIAs on newly created or recently modified systems of records. Although some work has been done in this area, the agency has no definitive plan in place to review the other existing eligible systems of records.

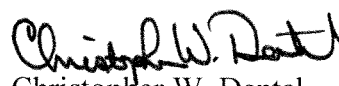
The CPSC has developed a mandatory training policy to attempt to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations and policies, and understand the ramifications of inappropriate access and disclosure. The training was prepared and made available to employees in a timely fashion; however, this program lacks adequate controls to verify whether or not employees actually took the training, much less whether or not they benefited from it.

In addition to the training policy detailed above, the CPSC has a policy that requires managers and supervisors to provide job-specific privacy training for all employees and contractors who in the course of their duties work with systems (in any medium) containing personally identifiable information. There has been no review and verification that System owners, managers, and supervisors are actually providing this training, much less a measure of its effectiveness, and much anecdotal evidence that would suggest that they are not. At least

some of the managers who were aware of this training requirement reported being unable to find suitable courses to meet the requirement.

Similarly, although there is an agency policy requiring agency managers and supervisors to review the internal controls relied upon to provide information security, adequate training regarding this requirement has not been provided to managers. This internal control is now (for the first time this year) certified in the agencies annual letters of assurance, but no independent review of the accuracy or effectiveness of this policy has been implemented to date.

Possibly as a result of the shortcomings in the privacy training program detailed above, the agency has had a number of recent incidents in which either the physical security of PII was compromised (Privacy Act protected data left unsecured) or PII data of third parties contained in death certificates, reports of injury, etc (social security numbers, addresses, phone numbers, etc) was made available (via the CPSC intranet) to all CPSC employees rather than being redacted before the reports in question were entered into an agency database.


Christopher W. Dentel
Inspector General

Chief Information Officer

Section Report

2009

Annual FISMA
Report

Consumer Product Safety Commission

For Official Use Only

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

1. Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your Agency but owned by another federal Agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

2. For the Total Number of Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		FISMA Inventory				Certification and Accreditation (C&A) and Testing					
		1a. Agency Systems	1b. Contractor Systems	1c. Systems owned by another Federal Agency	1d. Total Systems	2a. Number of systems certified and accredited		2b. Number of systems for which security controls have been tested and reviewed in the past year		2c. Number of systems for which contingency plans have been tested in accordance with policy	
Agency/ Component	Category	Number	Number	Number	Total Number	Total Number	% of Total	Total Number	% of Total	Total Number	% of Total
CPSC	High	0	0	2	0	0	0	0	0	0	0
	Moderate	1	0	1	1	1	100	1	100	0	0
	Low	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0
	Sub Total	1	0	3	1	1	100	1	100	0	0
Agency Totals	High	0	0	2	0	0	0	0	0	0	0
	Moderate	1	0	1	1	1	100	1	100	0	0
	Low	0	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0	0
	Total Systems	1	0	3	1	1	100	1	100	0	0

Question 3: Implementation of Security Controls in NIST Special Publication 800-53

What tools and techniques do you use for continuous monitoring?

Tool/Technique Name	Tool Category
ISS RealSecure	Intrusion Detection and Prevention Systems
Zen Asset Management	Inventory Management and Control Tool
eEye Retina	Vulnerability Scanners
Observation	Other
Hands-on control testing	Other

Question 4: Incident Detection, Monitoring and Reponse Capabilities

4a. What tools, techniques, technologies, etc., does the Agency use for incident detection?

Tool/Technique Name	Tool Category
Symantec Antivirus	Antimalware Software
Kaspersky Client Security	Antimalware Software
ISS Intrusion Detection	Intrusion Detection and Prevention Systems
Zen Asset Management	Inventory Management and Control Tool
CheckPoint Firewall	Network Access Control
Blue Coat Internet Scanner	Network Monitoring Software
eEye Retina	Vulnerability Scanners

4b. How many systems (or networks of systems) are protected using the tools, techniques and technologies described in 4(a) above?

1

4c. How often does the Agency log and monitor activities involving access to and modification of critical information?

0 % to 0 %

4d. What percentage of systems maintain audit trails that provide a trace of user actions?

0 % to 0 %

4e. Does the Agency maintain an incident handling and response capability?

Yes

4f. If the answer to 4(e) is yes, what percentage of systems are operated within the Agency's incident handling and response capability?

100 % to 100 %

4g. What tools, techniques, technologies, etc., does the Agency use for incident handling and response?

Tool/Technique Name	Tool Category
Symantec	Antimalware Software
Kaspersky Client Security	Antimalware Software
F-Secure	Antimalware Software
eEye Retina	Computer Forensic Tools
Nessus	Computer Forensic Tools
ISS Real Secure	Intrusion Detection and Prevention Systems
Blue Coat	Network Monitoring Software
Fluke Networks Sniffer	Network Monitoring Software

Question 5: Security Awareness Training

5a. Report the following for your Agency:

5a(1). Total number of people with log-in privileges to Agency systems.

555

5a(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

437 (79%)

5a(3). Number of people with log-in privileges to Agency systems that received information security awareness training using an ISSLOB shared service center. (Breakout total for b.)

0 (0%)

5a(4). Total number of employees with significant information security responsibilities.

25

5a(5). Number of employees with significant security responsibilities that received specialized training as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role-and Performance-Based Model".

23 (92 %)

5a(6). Total costs for providing information security training in the past fiscal year (in \$'s).

\$6,600

5b. Briefly describe the training provided in 5a(2) and 5a(5) and how you measure its effectiveness:

Comments:

The CPSC IT security awareness training course explains proper rules of behavior for the use of CPSC IT systems and information. It also explains common security threats and vulnerabilities. Effectiveness is measured through the use of course quizzes.

Question 6: Peer-to-Peer File Sharing

Does the Agency explain policies regarding the use of peer-to-peer file sharing in information security awareness training, ethics training, or any other Agency-wide training?

No

Question 7: Configuration Management

7a. Is there an Agency-wide configuration policy?

No

7a(1). Enter the systems/platforms/applications for which configuration policies exist and provide the implementation status.

Identify all that are applicable.

OS/Platform/System	Implementation Status
N/A	What tools and techniques is your Agency using for monitoring compliance?

OS/Platform/System	Implementation Status					
N/A	<table border="1"> <thead> <tr> <th data-bbox="978 139 1434 183">Tool/Technique Name</th> <th data-bbox="1434 139 1919 183">Tool Category</th> </tr> </thead> <tbody> <tr> <td data-bbox="978 183 1434 227"></td> <td data-bbox="1434 183 1919 227"></td> </tr> </tbody> </table>		Tool/Technique Name	Tool Category		
Tool/Technique Name	Tool Category					

7b. Indicate the status of the implementation of FDCC at your Agency:

7b(1). Agency has documented deviations from FDCC standard configuration.

No

7b(2). New Federal Acquisition Regulation 2008-004 language, which modified "Part 39-Acquisition of Information Technology," is included in all contracts related to commons security settings.

No

7b(3). List the percentage of workstations and laptops that are in compliance.

90 % to 100 %

Question 8: Systems Incident Reporting

Indicate whether or not the Agency follows documented policies and procedures for reporting incidents internally, to US-CERT and to law enforcement.

8a. How often does the Agency follow documented policies and procedures for identifying and reporting incidents internally?

90 % to 100 %

8b. How often does the Agency comply with documented policies and procedures for timelines of reporting to US-CERT?

90 % to 100 %

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement?

90 % to 100 %

Question 9: Performance Metrics for Security Policies and Procedures

Please provide three (3) outcome/output-based performance metrics your Agency uses to measure the effectiveness or efficiency of security policies and procedures. The metrics must be different than the ones used in these FISMA reporting instructions, and can be tailored from NIST's Special Publication 800-55 "Performance Measurement Guide for Information Security."

Metric Name	Metric Description
System and Communication	Measures the percentage of mobile computers and devices that perform all cryptographic operations using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.
Physical Security Incidents	Measures the percentage of physical security incidents allowing unauthorized entry into facilities containing information systems.
Incident Response	Measures the percentage of incidents reported within required time frame per applicable incident category.

Question 10: HSPD-12

Number of FISMA applications in which Federal employees and contractors are using HSPD-12 Personal Identity Verification credentials for access.

0

Inspector General

Section Report

2009

Annual FISMA
Report

Consumer Product Safety Commission

For Official Use Only

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

1. Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high) reviewed.

2. For the Total Number of Reviewed Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2		
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems(Agency and Contractor systems)		a. Number of systems certified and accredited	b. Number of systems for which security controls have been tested and reviewed in the past year	c. Number of systems for which contingency plans have been tested in accordance with policy
Agency/Component	Category	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed			
CPSC	High	0	0	0	0	0	0	0	0	0
	Moderate	1	1	0	0	1	1	1	1	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Sub Total	1	1	0	0	1	1	1	1	0
Agency Totals	High	0	0	0	0	0	0	0	0	0
	Moderate	1	1	0	0	1	1	1	1	0
	Low	0	0	0	0	0	0	0	0	0
	Not Categorized	0	0	0	0	0	0	0	0	0
	Total Systems	1	1	0	0	1	1	1	1	0

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The Agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and Agency policy.

Agencies are responsible for ensuring the security of information systems used by a contractor of their Agency or other organization on behalf of their Agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal Agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

3a. Does the Agency have policies for oversight of contractors?

No

3b. Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?

Yes

3c. Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?

No

3d. Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?

Yes

3e. The Agency inventory is maintained and updated at least annually.

No

3f. The IG generally agrees with the CIO on the number of Agency-owned systems.

Yes

3g. The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency.

Yes

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the Agency has developed, implemented, and is managing an Agency-wide plan of action and milestones (POA&M) process, providing explanatory detail in the area provided.

4a. Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?

Yes

4a(1). Has the Agency fully implemented the policy?

No

4b. Is the Agency currently managing and operating a POA&M process?

Yes

4c. Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency?

Yes

4d. Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?

Yes

4e. When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?

No

4f. For Systems Reviewed:

4f(1). Are deficiencies tracked and remediated in a timely manner?

No

4f(2). Are the remediation plans effective for correcting the security weakness?

No

4f(3). Are the estimated dates for remediation reasonable and adhered to?

No

4g. Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?

No

4h. Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?

No

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the Agency's certification and accreditation (C&A) process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" for C&A work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

5a. Has the Agency developed and documented an adequate policy for establishing a C&A process that follows the NIST framework?

No

5b. Is the Agency currently managing and operating a C&A process in compliance with its policies?

No

5c. For Systems reviewed, does the C&A process adequately provide:

5c(1). Appropriate risk categories

Yes

5c(2). Adequate risk assessments

Yes

5c(3). Selection of appropriate controls

Yes

5c(4). Adequate testing of controls

Yes

5c(5). Regular monitoring of system risks and the adequacy of controls

Yes

5d. For systems reviewed, is the Authorizing Official presented with complete and reliable C&A information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?

Yes

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

Provide a qualitative assessment of the Agency's process, as discussed in the SAOP section, for protecting privacy-related information, including adherence to existing policy, guidance and standards. Provide explanatory information in the area provided.

6a. Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?

Yes

6b. Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?

No

6c. Has the Agency developed and documented an adequate policy for PIAs?

Yes

6d. Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIAs?

No

Question 7: Configuration Management

7a. Is there an Agency wide security configuration policy?

No

7a(1). For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.

OS/Platform/System	Implementation Status				
N/A	<p data-bbox="863 305 1787 334">What tools and techniques is your Agency using for monitoring compliance?</p> <table border="1" data-bbox="968 345 1906 440"> <thead> <tr> <th data-bbox="974 352 1425 391">Tool/Technique Name</th> <th data-bbox="1425 352 1900 391">Tool Category</th> </tr> </thead> <tbody> <tr> <td data-bbox="974 391 1425 440"></td> <td data-bbox="1425 391 1900 440"></td> </tr> </tbody> </table>	Tool/Technique Name	Tool Category		
Tool/Technique Name	Tool Category				

7b. Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your Agency:

7b(1). Agency has documented deviations from FDCC standard configuration.

No

7b(2). New Federal Acquisition Regulation 2008-004 language, which modified "Part 39-Acquisition of Information Technology," is included in all contracts related to common security settings.

No

Question 8: Incident Reporting

8a. How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally?

100 % to 100 %

8b. How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT?

100 % to 100 %

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement?

100 % to 100 %

Question 9: Security Awareness Training

Provide an assessment of whether the Agency has provided IT security awareness training to all users with log-in privileges, including contractors. Also provide an assessment of whether the Agency has provided appropriate training to employees with significant IT security responsibilities.

9a. Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training?

Yes

9b. Report the following for your Agency:

9b(1). Total number of people with log-in privileges to Agency systems.

555

9b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

437 (79 %)

9b(3). Total number of employees with significant information security responsibilities.

25

9b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model."

23 (92 %)

Question 10: Peer-to-Peer File Sharing

10. Does the Agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training?

No

Senior Agency Official for Privacy

Section Report

2009

Annual FISMA
Report

Consumer Product Safety Commission

For Official Use Only

Question 1: Information Security Systems

Identify the number of Agency and contractor systems that contain Federal information in identifiable form. Identify the number of Agency and contractor systems for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act and identify the number of Agency and contractor systems covered by an existing PIA. Please identify the number of systems for which a system of records notice (SORN) is required under the Privacy Act and identify the number of systems for which a current SORN has been published in the Federal Register.

Agency / Component	a.			b.			c.				d.			e.			
	Number of systems that contain Federal information in identifiable form			Number of systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act			Number of systems in (b) covered by an existing PIA				Number of systems in (a) for which a system or records notice (SORN) is required under the Privacy Act			Number of systems in (d) for which a current SORN has been published in the Federal Register			
	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Number	Agency Systems	Contractor Systems	Total Number.	% Complete	Agency Systems	Contractor Systems	Total Number.	Agency Systems	Contractor Systems	Total Number	% Complete
CPSC	22	0	22	13	0	13	2	0	2	15%	22	0	22	21	0	21	95%
Total	22	0	22	13	0	13	2	0	2	15%	22	0	22	21	0	21	95%

Question 2: Links to PIAs and SORNS

2a. The URL of the centrally located page on the Agency web site listing working links to Agency PIAs.

<http://www.cpsc.gov/cpsc/pub/pubs/reports.html#pia>

2b. The URL of the centrally located page on the Agency web site listing working links to the published SORNS.

<http://www.cpsc.gov/cpsc/pub/pubs/systems.html>

Question 3: Senior Agency Official for Privacy (SAOP) Responsibilities

3a. Can your Agency demonstrate through documentation that the privacy official participates in all Agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)?

No

3b. Can your Agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19?

No

3c. Can your Agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information?

Yes

Question 4: Information Privacy Training and Awareness

4a. Does your Agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations and policies, and understand the ramifications of inappropriate access and disclosure?

Yes

4b. Does your Agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities?

No

Question 5: PIA and Web Privacy Policies and Processes

Does the Agency have a written policy or process for each of the following?

5a. PIA Policies

5a(1). Determining whether a PIA is needed.

Yes

5a(2). Conducting a PIA.

Yes

5a(3). Evaluating changes in business process or technology that the PIA indicate as necessary.

No

5a(4). Ensuring systems owners and privacy and IT experts participate in conducting the PIA.

Yes

5a(5). Making PIAs available to the public in the required circumstances.

Yes

5a(6). Making PIAs available in other than required circumstances.

No

5b. Web Policies

5b(1). Determining continued compliance with stated web policies.

No

5b(2). Requiring machine-readability of public-facing Agency web sites (i.e. use of P3P).

No

Question 6: Reviews Mandated by Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007

Component / Bureau	a. Section M Contracts	b. Records Practices	c. Routine Uses	d. Exemp- tions	e. Matching Programs	f. Training	g. Violations: Civil Action	h. Violations: Remedial Action	i. System of Record	j. (e)(3) Statement	k. Privacy Impact Assessments and Updates	l. Data Mining Impact Assessment
CPSC	No	No	No	0	1	No	No	No	21	0	7	No

Question 7: Written Privacy Complaints

In the table provided, indicate the number of written complaints for each type of of privacy issue allegation received by the SAOP, in addition to the number of complaints for each type of complaint. Written complaints do not include Freedom of Information Act requests or Privacy Act access requests.

Type of Complaint	Number of Complaints
7a. Process and Procedural - consent, collection, and appropriate notice.	0
7b. Redress - non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters.	0
7c. Operational - inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction.	0
7d. Referrals - complaints referred to another Agency with jurisdiction.	0

Question 8: Policy Compliance Review

8a. Does the Agency have current documentation demonstrating review of compliance with information privacy laws, regulations, and policies?

No

8b. Can the Agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?

Yes

8c. Does the Agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices?

No

8d. Does the Agency coordinate with the Agency's Inspector General on privacy program oversight?

Yes

Question 9: Information About Advice Provided by the SAOP

Please state “Yes” or “No” to indicate if the SAOP has provided formal written advice in each of the listed categories, and briefly describe the advice. For descriptions of training, please provide the number of employees (or contractors) who participated in the training.

9a. Agency policies, orders, directives, or guidance governing Agency handling of personally identifiable information.

Yes

9b. Written Agreements (either Interagency or with Non-Federal Entities).

No

9c. Reviews or feedback outside of the SORN and PIA process (e.g. formal written advice in the context of a budgetary or programmatic planning).

No

9d. Privacy Training (either stand-alone or included with training on related issues).

Stand Alone

Question 10: Agency Use of Persistent Tracking Technology

10a. Does the Agency use persistent tracking technology on any web site?

No

10b. Does the Agency annually review the use of persistent tracking?

No

10c. Can the Agency demonstrate through documentation the continued justification for, and approval to use, the persistent tracking technology?

No

10d. Can the Agency provide the notice language or citation for the web privacy policy that informs visitors about the persistent tracking?

No

Question 11: Privacy Points of Contact Information

Title / Role	Name	Phone	E-Mail
Agency Head	Inez Tenenbaum	301-504-7896	itenenbaum@cpsc.gov
Chief Information Officer	Patrick Weddle	301-504-7654	pweddle@cpsc.gov
Chief Information Security Officer	Patrick Manley	301-504-6946	pmanley@cpsc.gov
Senior Agency Official for Privacy	Mary Kelsey	301-504-7213	mkelsey@cpsc.gov
Agency Inspector General	Christopher Dentel	301-504-7644	cdentel@cpsc.gov
Chief Privacy Officer	N/A		
Privacy Advocate	Linda Glatz	301-504-7671	lglatz@cpsc.gov

Title / Role	Name	Phone	E-Mail
Privacy Act Officer	Todd Stevenson	301-504-6836	tstevenson@cpsc.gov
Reviewing Official for PIAs	Patrick Weddle	301-504-7654	pweddle@cpsc.gov
POC for URL links provided in Question 2	Philip Margolies	301-504-6987	pmargolies@cpsc.gov



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
WASHINGTON, DC 20207

PLF.

Memorandum

Date: October 1, 2008

TO : Kathleen Buttrey, Director, EO
Christopher Dentel, IG
Robert Howell, Deputy Acting AED, EXHR
John Horner, Director, CR
Cheryl A. Falvey, GC
John G. Mullan, AED, EXC
Richard O'Brien, Director, EXIP
Edward Quist, Director, EXFM
Donna Simpson, Director, EXRM
Julie Vallese, Director, EXPA

FROM : Patricia Semple ^{PS}
Executive Director

SUBJECT : Review of Systems Containing Personally Identifiable Information (PII) and
Review of Records Disposition Schedules

Last year, the Agency responded to requirements mandated by the Office of Management and Budget (OMB) to develop and implement a plan that would protect personally identifiable information (PII). Following OMB guidelines, we conducted an inventory of all systems that collect and retain PII (e.g., social security numbers, names, addresses, email addresses, telephone numbers, etc.) which can be used to identify an individual. Last year's efforts in this area provided the Agency with a strong start in completing the remaining OMB requirements regarding the protection of PII. In addition to PII requirements, all Federal agencies are required to update their Records Disposition Schedules and to insure that electronic records are included. Since these two efforts are so closely related and in an effort to save staff resources, I am asking that both efforts be completed simultaneously.

The Division of IT Policy and Planning (ITPP) of the Office of Information and Technology Services (EXIT) will be coordinating this effort. ITPP staff will be available to assist you in these efforts. I am asking each Office/Directorate to review the point of contact list attached and if necessary, identify a new point of contact within your organization to work with the ITPP to complete these requirements. Please provide your point of contact name to Linda Glatz, x7671, lglatz@cpsc.gov by October 8, 2008. An informational meeting will be held with all points of contact on October 22, 2008.

Following are the activities that must be completed (schedule attached): For personally identifiable information, agencies are required to 1) maintain an inventory of all systems containing PII, 2) identify systems that use social security numbers and eliminate the unnecessary use of social security numbers where possible, 3) identify possible systems of records, 4) conduct Privacy Impact Assessments as needed, 5) identify collections of information

in identifiable form for 10 or more persons subject to Paperwork Reduction Act, and 6) ensure that staff are trained on the proper use and handling of protected information and understand the steps to take if a breach occurs. For records disposition schedules, agencies are required to 1) make sure current schedules are accurate and 2) include electronic records in their schedules.

Each office is responsible for identifying systems containing PII and ensuring appropriate procedures are in place to safeguard these systems. Office managers will be asked to verify that they are meeting these requirements in their annual letters of assurance, beginning in 2009.

The following outlines the reviews required by your organization, suggestions for completing the process, and contact names for further information.

1) Develop Inventory of PII

Personally identifiable information (PII) refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. PII can be collected and maintained in any agency approved medium including electronic systems and hard copy paper files that directly identify an individual. Examples of PII include: name, social security number, date of birth, financial records, email address, phone number, home address, driver's license number, etc. Work-related phone numbers, street address, email address, and employment information such as present and past position titles, occupational series, grades, salary rates, etc. are not considered PII unless covered by a Privacy Act System of Records. CPSC's PII Policy is found in Directive 1435.1, Policies and Procedures Pursuant to the Privacy Act.

Every agency is to maintain an inventory of systems containing PII. A preliminary effort to gather this information was previously made with each office. (See Tab A for results) This information should be reviewed and updated as necessary. Unnecessary systems should be eliminated. For now, we have the information in a data base, but in the future we anticipate an online, interactive system that will allow you to make changes as needed to keep the inventory up to date.

Systems that are unique to an individual and have no official CPSC use, such as personal rolodexes, should not be identified on this inventory. A completed PII inventory will help in identifying further actions needed for systems that may have social security numbers, need privacy impact assessments, or are subject to Paperwork Reduction Act, therefore, this should be your first step and should be completed by December 22, 2008.

Linda Glatz, ITPP, x7671, is available to receive your PII inventory and assist you with the process.

2) Identify Systems with Social Security Numbers (SSNs)

Review each system in your PII inventory (see step 1) that includes the use of SSNs. If the use of SSNs can be eliminated from any of these systems, please identify the system and the date that use of SSNs will be eliminated. CPSC must report on the number of systems where the use of SSN's has been eliminated. Please provide this information to Linda Glatz, ITPP, x7671 by January 8, 2008.

3) Review existing Systems of Records and identify new Systems of Records

A System of Records is a group of records that contains a personal identifier (e.g., name, social security number) and it contains at least one other personal data element (e.g., financial information, spouse name, medical information, etc.) AND the file is retrieved by a personal identifier. All SORs require a notice in the Federal Register. The Privacy Act of 1974 requires agencies to follow certain procedures for collecting and safeguarding information in a System of Records.

CPSC has identified a number of Systems of Records. A listing appears in CPSC Order 1435.1, Appendix 1 and on our web site. (See Tab B.)

Review each System of Records that your organization is responsible for and make sure the information is still accurate. Note any further changes needed and provide this information to Linda Glatz by December 22, 2008.

Next, review your PII inventory and determine if there may be systems that should be identified as possible new Systems of Records. Changes to existing systems and possible new systems should be identified. Additional guidance pertaining to definitions of records and Systems of Records as well as opinions concerning systems used to log/track work can be found in the OGC memorandum at Tab C. All new SORs should be identified and an FR notice prepared by January 22, 2009.

4) Conduct Privacy Impact Assessments as needed

A Privacy Impact Assessment (PIA) is a checklist or tool to ensure that new or modified collections of information on individuals are evaluated for privacy risks. Each system owner is responsible for developing a PIA. All electronic systems containing PII should have a Privacy Impact Assessment completed by February 27, 2009. No PIA is required where information relates to internal government operations (e.g., web site where system does not collect or maintain information identifiable about the public.) PIAs are made publicly available on the CPSC web site.

The CPSC Privacy Impact Assessment Policy can be found at Directive 1435.6. CPSC has developed a template and guidance for conducting a PIA. These documents can be found at <https://cpscnet.cpsc.gov/it/privacy/piatemplate.doc> and <https://cpscnet.cpsc.gov/it/privacy/pia.doc>. Contact Linda Glatz, ITTPP, x7671 for more information.

5) Identify Collections subject to Paperwork Reduction Act Requirements

Identify collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government) that are subject to the requirements of the Paperwork Reduction Act (PRA). Obtain clearance from the Office of Management and Budget for the information collection. If the collection is electronic, then a PIA is also required. Contact Linda Glatz, x7671, for further information.

6) Conduct Staff Training

All agency managers are responsible for developing, administering, monitoring, and enforcing internal controls, including security controls, within their areas of authority. This includes operating procedures for the handling of PII and Systems of Records and training staff on the use and protection of the information. These responsibilities will be addressed in the annual letters of assurance.

“CPSC Privacy Awareness Training” is online training available at <https://cpscnet.cpsc.gov/it/privacy/privacytraining.ppt> Each employee is required to review the Privacy Training annually and an email will be sent to all employees October 1, 2008 reminding them of this requirement. Supervisors will be asked to certify by November 31, 2008, that their employees have completed the Privacy training. Employees and their supervisors must also sign a document annually that clearly describes their understanding of their responsibilities and potential consequences for breach of PII (Information Systems Rules of Behavior). Further information about protection of personally identifiable information can be found at Tab D, Draft Management Instruction: Protection of Personally Identifiable Information Control for CPSC Agency and Mission Critical Systems.

7) Review of Records Disposition Schedules

Identify all records systems in your organization and the records disposition schedule for each. Electronic records created and received by agencies are subject to the same existing statutory and regulatory records management requirements as records in other formats and on other media. For a copy of the current records schedule see <https://em.cpsc.gov/cpscpriv/recmgmt/CPSCDispositionofRecords.doc>. For more information about applying schedules for your specific records needs, contact Cheryl John, x6917, cjohn@cpsc.gov. Your review of your records disposition schedule should be completed by January 31, 2009.



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
WASHINGTON, DC 20207

PLF.

Memorandum

Date: October 1, 2008

TO : Kathleen Buttrey, Director, EO
Christopher Dentel, IG
Robert Howell, Deputy Acting AED, EXHR
John Horner, Director, CR
Cheryl A. Falvey, GC
John G. Mullan, AED, EXC
Richard O'Brien, Director, EXIP
Edward Quist, Director, EXFM
Donna Simpson, Director, EXRM
Julie Vallese, Director, EXPA

FROM : Patricia Semple ^{PS}
Executive Director

SUBJECT : Review of Systems Containing Personally Identifiable Information (PII) and
Review of Records Disposition Schedules

Last year, the Agency responded to requirements mandated by the Office of Management and Budget (OMB) to develop and implement a plan that would protect personally identifiable information (PII). Following OMB guidelines, we conducted an inventory of all systems that collect and retain PII (e.g., social security numbers, names, addresses, email addresses, telephone numbers, etc.) which can be used to identify an individual. Last year's efforts in this area provided the Agency with a strong start in completing the remaining OMB requirements regarding the protection of PII. In addition to PII requirements, all Federal agencies are required to update their Records Disposition Schedules and to insure that electronic records are included. Since these two efforts are so closely related and in an effort to save staff resources, I am asking that both efforts be completed simultaneously.

The Division of IT Policy and Planning (ITPP) of the Office of Information and Technology Services (EXIT) will be coordinating this effort. ITPP staff will be available to assist you in these efforts. I am asking each Office/Directorate to review the point of contact list attached and if necessary, identify a new point of contact within your organization to work with the ITPP to complete these requirements. Please provide your point of contact name to Linda Glatz, x7671, lglatz@cppsc.gov by October 8, 2008. An informational meeting will be held with all points of contact on October 22, 2008.

Following are the activities that must be completed (schedule attached): For personally identifiable information, agencies are required to 1) maintain an inventory of all systems containing PII, 2) identify systems that use social security numbers and eliminate the unnecessary use of social security numbers where possible, 3) identify possible systems of records, 4) conduct Privacy Impact Assessments as needed, 5) identify collections of information

in identifiable form for 10 or more persons subject to Paperwork Reduction Act, and 6) ensure that staff are trained on the proper use and handling of protected information and understand the steps to take if a breach occurs. For records disposition schedules, agencies are required to 1) make sure current schedules are accurate and 2) include electronic records in their schedules.

Each office is responsible for identifying systems containing PII and ensuring appropriate procedures are in place to safeguard these systems. Office managers will be asked to verify that they are meeting these requirements in their annual letters of assurance, beginning in 2009.

The following outlines the reviews required by your organization, suggestions for completing the process, and contact names for further information.

1) Develop Inventory of PII

Personally identifiable information (PII) refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. PII can be collected and maintained in any agency approved medium including electronic systems and hard copy paper files that directly identify an individual. Examples of PII include: name, social security number, date of birth, financial records, email address, phone number, home address, driver's license number, etc. Work-related phone numbers, street address, email address, and employment information such as present and past position titles, occupational series, grades, salary rates, etc. are not considered PII unless covered by a Privacy Act System of Records. CPSC's PII Policy is found in Directive 1435.1, Policies and Procedures Pursuant to the Privacy Act.

Every agency is to maintain an inventory of systems containing PII. A preliminary effort to gather this information was previously made with each office. (See Tab A for results) This information should be reviewed and updated as necessary. Unnecessary systems should be eliminated. For now, we have the information in a data base, but in the future we anticipate an online, interactive system that will allow you to make changes as needed to keep the inventory up to date.

Systems that are unique to an individual and have no official CPSC use, such as personal rolodexes, should not be identified on this inventory. A completed PII inventory will help in identifying further actions needed for systems that may have social security numbers, need privacy impact assessments, or are subject to Paperwork Reduction Act, therefore, this should be your first step and should be completed by December 22, 2008.

Linda Glatz, ITPP, x7671, is available to receive your PII inventory and assist you with the process.

2) Identify Systems with Social Security Numbers (SSNs)

Review each system in your PII inventory (see step 1) that includes the use of SSNs. If the use of SSNs can be eliminated from any of these systems, please identify the system and the date that use of SSNs will be eliminated. CPSC must report on the number of systems where the use of SSN's has been eliminated. Please provide this information to Linda Glatz, ITPP, x7671 by January 8, 2008.

3) Review existing Systems of Records and identify new Systems of Records

A System of Records is a group of records that contains a personal identifier (e.g., name, social security number) and it contains at least one other personal data element (e.g., financial information, spouse name, medical information, etc.) *AND* the file is retrieved by a personal identifier. All SORs require a notice in the Federal Register. The Privacy Act of 1974 requires agencies to follow certain procedures for collecting and safeguarding information in a System of Records.

CPSC has identified a number of Systems of Records. A listing appears in CPSC Order 1435.1, Appendix 1 and on our web site. (See Tab B.)

Review each System of Records that your organization is responsible for and make sure the information is still accurate. Note any further changes needed and provide this information to Linda Glatz by December 22, 2008.

Next, review your PII inventory and determine if there may be systems that should be identified as possible new Systems of Records. Changes to existing systems and possible new systems should be identified. Additional guidance pertaining to definitions of records and Systems of Records as well as opinions concerning systems used to log/track work can be found in the OGC memorandum at Tab C. All new SORs should be identified and an FR notice prepared by January 22, 2009.

4) Conduct Privacy Impact Assessments as needed

A Privacy Impact Assessment (PIA) is a checklist or tool to ensure that new or modified collections of information on individuals are evaluated for privacy risks. Each system owner is responsible for developing a PIA. All electronic systems containing PII should have a Privacy Impact Assessment completed by February 27, 2009. No PIA is required where information relates to internal government operations (e.g., web site where system does not collect or maintain information identifiable about the public.) PIAs are made publicly available on the CPSC web site.

The CPSC Privacy Impact Assessment Policy can be found at Directive 1435.6. CPSC has developed a template and guidance for conducting a PIA. These documents can be found at <https://cpscnet.cpsc.gov/it/privacy/piatemplate.doc> and <https://cpscnet.cpsc.gov/it/privacy/pia.doc>. Contact Linda Glatz, ITTPP, x7671 for more information.

5) Identify Collections subject to Paperwork Reduction Act Requirements

Identify collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government) that are subject to the requirements of the Paperwork Reduction Act (PRA). Obtain clearance from the Office of Management and Budget for the information collection. If the collection is electronic, then a PIA is also required. Contact Linda Glatz, x7671, for further information.

6) Conduct Staff Training

All agency managers are responsible for developing, administering, monitoring, and enforcing internal controls, including security controls, within their areas of authority. This includes operating procedures for the handling of PII and Systems of Records and training staff on the use and protection of the information. These responsibilities will be addressed in the annual letters of assurance.

“CPSC Privacy Awareness Training” is online training available at <https://cpscnet.cpsc.gov/it/privacy/privacytraining.ppt> Each employee is required to review the Privacy Training annually and an email will be sent to all employees October 1, 2008 reminding them of this requirement. Supervisors will be asked to certify by November 31, 2008, that their employees have completed the Privacy training. Employees and their supervisors must also sign a document annually that clearly describes their understanding of their responsibilities and potential consequences for breach of PII (Information Systems Rules of Behavior). Further information about protection of personally identifiable information can be found at Tab D, Draft Management Instruction: Protection of Personally Identifiable Information Control for CPSC Agency and Mission Critical Systems.

7) Review of Records Disposition Schedules

Identify all records systems in your organization and the records disposition schedule for each. Electronic records created and received by agencies are subject to the same existing statutory and regulatory records management requirements as records in other formats and on other media. For a copy of the current records schedule see <https://em.cpsc.gov/cpscpriv/recmgmt/CPSCDispositionofRecords.doc>. For more information about applying schedules for your specific records needs, contact Cheryl John, x6917, cjohn@cpsc.gov. Your review of your records disposition schedule should be completed by January 31, 2009.