U.S. CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

REPORT

September 22, 2006

Federal Information Security Management Act Report
Table of Contents

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 follow-ups to it done in 2002, 2003 and 2004 in conjunction with the independent reviews required by FISMA and audits with information technology aspects (CFO Act Audit, etc.) served as the basis for the IG's Fiscal Year 2005 evaluation.

The Fiscal Year 2005 FISMA IG independent evaluation found that substantial improvements have been made and all material weaknesses have been corrected. After those deficiencies that were found to be "material weaknesses" were addressed, the CPSC began the process of implementing the recommendation set out in previous evaluations to deal with less serious security deficiencies ("high" priority security vulnerabilities). All eleven of these "high" priority security vulnerabilities were also addressed. As a result of the work done in Fiscal Year 2004, the interim label was removed from the CPSC's system certification and accreditation.

This years FISMA evaluation found that although improvements continued to be made in the IT Security area, these improvements did not keep pace with the pace of the new requirements mandated by NIST. In particular funding was not available in FY 06 to complete the testing of system security controls mandated by NIST SP 800-53 and OMB policy. As a result the CPSC's system lost its certification and accreditation. However, corrective action has been taken and the system should regain certification and accreditation in FY 07.

Efforts are also still being made to bring the CPSC into full compliance with all other FISMA and OMB requirements and to address the remaining lower priority security requirements.

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

FEDERAL INFORMATION 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 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 to determine the effectiveness of such program and practices.

Scope and Methodology: The evaluation was conducted in August and September of 2006. 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.

This review took place in the form of both a follow-up of the findings and recommendations resulting from earlier audits and a review of the CPSC's implementation of recent IT security criteria issued by the National Institute of Standards and Technology. 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 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 has failed to accomplish all of the new (FY 06) 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 planing, 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.

Action 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 have been prepared. PEC has 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 this area have been 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 have been 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 are also still being made 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. Funds have currently been set aside and the procurement process initiated so that this will be accomplished in FY 07.

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 new ISSP was completed just before the end of FY 03. Implementation of the recommendations contained in the ISSP continued throughout FY 04, 05, and 06. Currently, 292 employees, seventy-two percent of CPSC staff, have completed security training. Full implementation of the ISSP, as funding allows, should result in even more effective information system security controls.

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 2003 and 2004 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 2002, 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 2003, CPSC committed $714,891 to this area in the form of salaries and other expenses. In FY 2004, CPSC committed $715,000 for its Information Technology programs. In FY 2005, this figure rose to $1,035,100. In FY 2006, the CPSC spent $2,082,050 on its IT programs. Work on implementing the recommendations contained in the ISSP continued throughout FY 04 and FY 05 (automatic database "snapshots" of the e-mail system, monitoring of Internet usage, etc. were all implemented). Full implementation of this plan, as funding allows, should result in even more effective information system security controls.

Plan of Action and Milestones: CPSC's most recent Plan of Action and Milestones report to the OMB reflects both the improvements that CPSC has made, it has now resolved both all material weaknesses as well as all "high" security vulnerabilities, and CPSC's acknowledgement of its need for continued improvement. Stated goals from FY 04 which were met in FY 05 include implementing a security awareness training program, providing a redundant cooling

capability to the Agency's existing computer room air conditioning unit, and 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. In FY 06, automated system auditing was implemented. Stated goals on which the CPSC continues to work include enabling the system to enforce strong user passwords, implementing network data port authentication, developing formal documented procedures for physical access control, and developing a formal agency wide security configuration policy.

Performance Measures: Security act 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.

Work is presently underway to incorporate NIST 800-53 controls. Agency personnel are working to ensure that future certification and accreditation work will be consistent with the new NIST Special Publication requirements.