Description of document:	Consumer Product Safety Commission (CPSC) Inspector General's (OIG) Consumer Product Safety Improvement Act (CPSIA) Annual Reports to Congress, FY 2011 – FY 2013
Request date:	2014
Released date:	22-December-2014
Posted date:	05-January-2015
Source of document:	FOIA Requester Service Center US Consumer Product Safety Commission 4330 East West Highway, Room 502 Bethesda, MD 20814 Fax: 301-504-0127 Email: cpsc-foia@cpsc.gov

U.S. CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

December 22, 2014

RE: Freedom of Information Act (FOIA) Request #15-F-00128: Request a copy of the Inspector General's Consumer Product Safety Improvement Act (CPSIA) Annual Report to Congress for the most recent five years

Thank you for your Freedom of Information Act (FOIA) request seeking information from the U.S. Consumer Product Safety Commission ("Commission"). Enclosed are copies of the report that you requested for Fiscal Years 2011, 2012 and 2013 respectively. The report for FY 2014 is not yet available.

This completes the processing of your request. The cost to the Commission to prepare this information was $40.00. In this case, we have decided to waive the charges. This completes the processing of your request. Should you have any questions, contact us by letter, facsimile (301) 504-0127, telephone (301) 504-7923, or e-mail addressed to cpsc-foia@cpsc.gov.

Sincerely,

Alberta E. Mills
Freedom of Information Officer
The Secretariat - Office of the Secretary
Office of the General Counsel

Enclosure

FISCAL YEAR 2011

Executive Summary

The Consumer Product Safety Improvement Act (CPSIA) of 2008 requires that the Office of Inspector General (OIG) of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the findings, conclusions, and recommendations from its reviews and audits performed under section 205(a) of the CPSIA and any relevant employee complaints under section 205(b) of the CPSIA. This report deals with the CPSC's capital improvement efforts involving information technology.

The CPSIA requires that the CPSC improve its information technology (IT) architecture in general, and that it establish and maintain a database on the safety of consumer products and other products or substances regulated by the Commission. The database must be publicly available, searchable, and accessible through the Internet website of the Commission. The development of this database constitutes, by a wide margin, the largest single IT project ever undertaken by the CPSC.

The purpose of the database is to provide a single central location where consumers can report incidents (known as Reports of Harm) and search for prior incidents/recalls. Additionally, the database provides the manufacturers, private labelers, and importers of the products in question with the ability to comment on the Reports of Harm submitted. For example, the manufacturer can use the comment functionality within the database to comment on actions taken to remediate product safety concerns or to rebut a Report of Harm. Moreover, if they believe that the information provided in a Report of Harm contains confidential information or is materially inaccurate, businesses can use the database to request that the CPSC correct Reports of Harm submitted by consumers.

The database is an integral part of the overall CPSC IT Modernization effort, known as the Consumer Product Safety Risk Management System (CPSRMS). The implementation of the CPSRMS will occur over the next few years, and as of January 18, 2011, it was estimated to cost approximately $67.6 million.[1]

Two reviews of the CPSRMS were conducted during the period covered by this report. The first of these was a Security Review and the second a review of the CPSRMS' compliance with section 212 of the Consumer Product Safety Improvement Act. A brief summary of each report follows:

[1] According to the Capital Asset Plan and Business Case Summary, provided to the OMB on January 18, 2011, the total estimated CPSRMS life cycle cost, including Steady State and Full-Time Equivalents costs, is $67,643,000. This amount includes actual amounts of $8,955,000 for 2009 and $11,476,000 for 2010; and estimated amounts of $11,980,000 for 2011; $10,316,000 for 2012; $7,440,000 for 2013; $5,784,000 for 2015, and $5,845,000 for 2015 and beyond. The estimated cost agreed to the President's Budget, submitted on January 18, 2011. According to the President's Budget, the total Agency funding for CPSRMS in FY 2010 was $10,135,000 for the Development, Modernization, and Enhancement costs and $1,341,000 for the Steady State costs.

Consumer Product Safety Risk Management System
Information Security Review Report

The U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conducted a compliance review of the implementation and establishment of the CPSC's publically available consumer product safety information database.

The CPSRMS houses personal, proprietary, and confidential data. As defined by NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the CPSRMS is categorized as a major application. Therefore, the CPSRMS is required to implement specific security controls and complete a Security Certification and Accreditation (C&A) separate from the CPSC General Support System (GSS LAN). NIST SP 800-37, *Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010 provides guidance and best practices for the C&A process that agencies are required to implement in accordance with the Federal Information Security Management Act (FISMA). CPSC management reviewed and validated the CPSRMS's system security through the performance of a C&A assessment and formally authorized the CPSRMS to operate on January 16, 2011.

To satisfy the NIST SP 800-37 requirements, the CPSC contracted with Communications Resources Inc. (CRI), an outside IT consultancy to perform the initial categorization, selection, and implementation of the CPSRMS security controls, and to develop the CPSRMS System Security Plan (SSP). Other deliverables provided by CRI included:

The CPSC contracted SecureIT to perform an independent security assessment of the CPSRMS implementation, and develop the SAR for the CPSRMS. SecureIT is also responsible for maintaining the CPSRMS SSP and developing the Continuous Monitoring Plan and the Asset Inventory Report.

Overall, the review found several inconsistencies and weaknesses in the way the CPSC initially executed the C&A process for the CPSRMS. These weaknesses stemmed primarily from a lack of organizational resources at the time of the CPSRMS' implementation; resulting in the heavy reliance on independent contractors for the development and implementation of the CPSRMS. At the time of the initial C&A process, the CPSC's lacked the mature organizational processes and the procedural documents required to ensure the adequate governance of the C&A process. As noted below, management has made substantial progress in addressing these findings.

Consumer Product Safety Improvement Act of 2008
Section 212 Statutory Compliance Audit

This audit, conducted in accordance with generally accepted government audit standards (GAGAS), covered the CPSC's implementation of the publically available consumer product safety information database, and assessed the database's compliance with Section 212 of the CPSIA. Overall, it was determined that the CPSC had substantially complied with the requirements of the CPSIA for the database. However, one instance was noted in which personal information regarding a consumer (name, contact, and medical information), was inadvertently made available to the public. The type of information in question is characterized by the government as Personally Identifiable Information (PII), and its actual or potential unauthorized release is referred to as a breach of PII.

This particular breach of PII occurred because the CPSC did not properly conceal or redact the PII contained in a publically available Report of Harm. The agency has now taken appropriate corrective action.

Office Relocations: Although a review of the agency's physical capital improvement efforts related to the relocation of offices at the CPSC HQ building was originally planned, this review was canceled. An unpublished survey of relocation efforts was conducted as a precursor to the review and the preliminary results of this survey were shared with senior management. However, due to problems with the methodology of the survey, a number of its findings were suspect and its results could not be used to develop a formal review or audit.

Introduction

This report has been prepared in accordance with the Consumer Product Safety Improvement Act (CPSIA) of 2008. The CPSIA constituted a comprehensive overhaul of consumer product safety rules, and it significantly impacted nearly all children's products entering the U.S. market.

The CPSIA also required that the Inspector General of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the Inspector General's findings, conclusions, and recommendations from any reviews or audits performed under subsections (a) "Improvements by the Commission" and (b) "Employee Complaints" of section 205 of the CPSIA.

This report fulfills the above-referenced requirements. The report focuses on the development of the database of publicly available information on incidents involving injury or death, required under section 6A of the Consumer Product Safety Act.

Consumer Product Safety Risk Management System Information Security Review Report:

The Consumer Product Safety Improvement Act of 2008 (CPSIA), P.L. 110-314, Section 212 requires the CPSC to implement a publicly accessible, searchable database of consumer product incident reports. Pursuant to section 6A(a)(3) of the CPSIA, the database had to be established within the 18-month period following the CPSC's submission of a plan to Congress regarding the Database implementation under section 6A(a)(2). The CPSC submitted this plan to Congress on September 10, 2009. Therefore, the Database launch date was set for March 11, 2011.

The Consumer Product Safety Risk Management System

The CPSC contracted with InfoReliance (IR) to begin the development of a solution to meet this legislative requirement for a public database. IR customized one of its Commercial-Off-The-Shelf (COTS) products to meet the requirements defined by the CPSIA/CPSC management and developed SaferProducts.gov. The purpose of this tool is to provide a single, central location where consumers can report incidents and search for prior incidents/recalls. Additionally, this tool provides the manufacturers of the products in question with an opportunity to comment on actions taken to remediate the product safety concerns, as well as rebut, correct, and add additional precision to such reports. Moreover, this tool is an integral part of the overall IT Modernization effort, termed CPSRMS.

The CPSRMS architecture includes a core development framework and three key applications using that framework: the Consumer/Public Portal, the Industry Partner Portal, and the Incident Management Control Center (IMCC). By customizing an existing COTS product, the CPSC did not have to develop and support an in-house solution and has the option to draw from an outside pool of experts for future support needs. However, historically the challenge with this type of implementation is integrating the COTS tool with the legacy solutions already in place. Therefore, in order to ensure the validity of the IR architectural documentation and identify

security vulnerabilities associated with the overall CPSRMS architecture, which includes the integration between the IR solution and the legacy systems already in place, the CPSC contracted with Aspect Security to perform an independent architectural security review. The scope of this review included the custom application components and related controls developed by the CPSC. Analysis of these custom application components and controls focused on the areas of Identity Management and Authentication, Session Management, Access Control, Input Validation and Output Encoding, and Sensitive Data Protection.

SUMMARY OF FINDINGS

At the time fieldwork was performed, there were several inconsistencies and weaknesses in the certification and accreditation (C&A) assessment of the CPSRMS. These weaknesses stemmed primarily from a lack of mature organizational processes and procedural documents required to ensure the adequate governance of the C&A process. In addition, management's lack of internal resources at the time of implementation played a significant part in the weaknesses identified in the C&A assessment. Management concurred with the majority of our findings and recommendations and indicated that work had been completed or was in progress to address many of the deficiencies found.

FINDING 1: The draft Risk Management Framework strategy had yet to be formalized or implemented.

At the time of fieldwork, a Risk Management Framework had been drafted, but not been implemented. As such, the CSPC had not formally implemented a Risk Executive (function). The CPSC Security team documented the CPSC Risk Management Framework based on the NIST SP 800-39 (Draft), *Managing Information Security Risk: Organization, Mission, and Information System View*, dated April 2008. NIST SP 800-39 outlined the proposed approach to addressing risk from an organizational perspective and it addresses most of the NIST SP 800-37 requirements. The implementation of the Risk Management Framework and the establishment of a Risk Executive (function) did not occur due to a lack of resources available to perform the required duties and a lack of management support for the creation of these organizational roles. Consequently, the tasks required in NIST SP 800-37 and NIST SP 800-39 were not being performed. Thus, there was a strong likelihood that the agency had not assigned the correct amount of effort/ resources to identifying, prioritizing, and mitigating agency risks.

Moreover, the CPSC did not document one of the topics that NIST SP 800-37 requires in the Risk Management strategy – the Organizational Risk Tolerance. Per CPSC management, the Organizational Risk Tolerance had not been defined or documented. For C&A purposes, management informally tied the Agency Organizational Risk Tolerance to the CPSRMS system categorization of "Moderate." The system categorization of "Moderate" was defined using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004. Management also documented the level of risk acceptable for CPSRMS to operate in the Authorization to Operate (ATO) document. The ATO document states that CPSRMS will not be authorized to operate if any "high-impact" security weaknesses are identified and unmitigated.

Recommendations:

1. Identify the participants in the CPSC Risk Executive Council, and then begin the top-down and bottom-up process of developing a risk management organization. A top down approach to developing a risk management organization requires senior management to identify the participants of the Executive Risk Council. A bottom up approach to developing the risk management organization requires the Executive Risk Council to identify the resources responsible to provide the relevant risk information within the organization. Additionally, require these resources, as outlined in the Risk Management Framework, to begin taking on the risk management responsibilities assigned to them.

2. Define specific tasks and milestones associated with implementing the proposed Risk Management Framework. Additionally, implement a process to track and quantify the aggregate risks from all Information Systems (*e.g.*, a risk heat map) and include this procedure in the Risk Management Framework. This should be led by the Risk Executive Function and tied to the Enterprise Architecture.

3. Senior CPSC management (*e.g.*, the Risk Executive Function) should define a methodology for developing the risk tolerance for the CPSC and formally establish an organizational tolerance for risk in the Risk Management Framework. The risk tolerance should be communicated and guidance provided to appropriate agency resources on how risk tolerance impacts ongoing decision making activities, as recommended by NIST SP 800-39 (Draft). Finally, management should update the Risk Assessment to include documentation of the risk tolerance and used to justify the ATO decisions going forward.

Management Response: Management generally concurred with this finding.

FINDING 2: The CPSC had not yet developed an Enterprise Architecture with Information Security considerations.

At the time of fieldwork, the CPSC had not yet developed an Enterprise Architecture with Information Security considerations; therefore, the information types and security controls had never been mapped to the Enterprise Architecture. This was due to the amount of effort required to document the Enterprise Architecture and the limited number of agency resources assigned to this effort. This led to the CPSC's inability to document properly the implementation of system-specific and hybrid security controls within the information system while taking into account specific technologies and platform dependencies. Additionally, the CPSRMS SSP states that the Information Security and Enterprise Architecture was scheduled to be implemented during FY 2010; however, that deadline passed without implementation. Without a comprehensive Enterprise Architecture, entire enterprise components (Segment and Solution Architectures) may go unidentified, and the weaknesses associated with these enterprise components may go un-remediated due to this lack of mapping and visibility.

Recommendation: Develop an Enterprise Architecture that includes a comprehensive IT Security Architecture using the CIO Counsel's guidance (FEA-Security-Privacy-Profile-v3-9-30-2010) and incorporate this into the relevant Security Control Documents. Additionally, all the security controls, including the controls required by NIST SP 800-53, *Revision 3 Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009, should be mapped to the Enterprise Architecture/Information Security Architecture to provide a comprehensive view of the security control relationships. Management can accomplish this through the development of Segment Architectures based on the primary CPSC mission objectives and business processes. Once the definition of segments occurs, a Solution Architecture should be designed for each of the individual segments. The Solution Architectures should include details that define each of the related security controls, including those defined in NIST SP 800-53. The Solution Architecture should also include mapping to the other Solution and Segment Architectures and with this view, controls should be classified as "Common," "Hybrid," or "System Specific." Controls defined as "Hybrid," should be included in all associated Solution/Segment Architectures to ensure that the control components are properly mapped to each of the participating systems. Controls defined as "Common" should be included (or referred to) in each of the associated Solution/Segment Architectures to provide a full view of the security of each of the Solutions and Segment Architectures. In addition, the Enterprise Architecture framework would be the most appropriate way to assign priority and criticality to each of the IT Systems in terms of "Confidentiality," "Integrity," and "Availability," as this process is not defined in any of the other Security Control Documents.

Management Response: Management concurred with this finding.

FINDING 3: Insufficient documentation of the implementation of NIST SP 800-53 security controls in the CPSRMS SSP.

At the time of fieldwork, the implementation of the NIST SP 800-53 security controls did not include sufficient detail of implementation in the CPSRMS SSP. This was due to a lack of management oversight of the CRI contract and management not effectively enforcing the stipulations set forth in the CRI Statement of Work. Without sufficient detail, the traceability to the decisions made prior to and after the deployment of the information system, as required by NIST SP 800-37, may not be possible. As such, we noted the following:

a) Individual documentation of the sub-controls and their implementation was not included; therefore, the CPSRMS SSP was unable to describe "*the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control.*" Moreover, the control developer/implementer did not provide a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control, as required by NIST 800-53. The implementation description included a description of the finding, if the control was deemed to be not fully compliant, or a high-level description of the control, if it was deemed to be in place; however, the control descriptions were not defined in terms of "Planned Inputs," "Expected Behavior," and "Expected Outputs," as required. Further, it was noted that a description that might be used to document "Minimum Assurance Requirements" was not documented. Although the SCIP documented unimplemented

controls in these terms, it contains only 12 security controls. However, there were 86 "Planned," "Partially Compliant," or "Noncompliant" controls that appeared in the SSP and 47 "Other than Satisfied" controls that appeared in the CPSRMS SAR. Additionally, the CPSRMS SAR did not include sufficient descriptions of any of the controls considered fully implemented.

b) Four controls: PM-10, SI-10, AU-9, and IA-8, were defined, as "Partially Compliant" in the CPSRMS SSP, but did not have an associated implementation strategy documented in the CPSRMS SSP; and were not separately documented in the SCIP or Risk Assessment. Instead, where this information should have been documented, the signification "None" appeared.

c) The documentation regarding tailoring of the baseline security controls, by applying scoping, parameterization, and compensating control guidance, was incomplete. For example, parameterization details such as configuration parameters; session timeout; registry settings; account, file, and directory settings (*i.e.* permissions, and settings for services, ports, protocols, and remote connections) were not documented in the CPSRMS SSP. In addition, guidance on how the agency plans to employ compensating controls was not documented in the CPSRMS SSP.

d) The documentation for the justification for adding 10 supplemental controls to the CPSRMS SSP was incomplete. As NIST SP 800-53 provisions for a moderate impact system did not require these controls, OMB A-130 states that the agency must "*Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications.*"

Recommendations:

1. Fully document the implementation of the security controls, including the implementation of the sub-controls, in the CPSRMS SSP with sufficient detail to facilitate the assessment of individual controls. This includes documenting specific actions that will be required to perform the control, as well as determining whether to accept that control is correctly designed and operating effectively by defining the Minimum Assurance Requirements. The CPSRMS SAR format is a more effective format to accomplish this than the one currently being used for the CPSRMS SSP.

2. Define all security controls assessed in the CPSRMS SSP/SAR assessments in terms of "Planned Inputs" (including cost and resources required), "Expected Behavior," and "Expected Outputs" within the CPSRMS SSP, SCIP, or Risk Assessment. If this is not to be documented directly in the text of the CPSRMS SSP, then the document that has this information should be included as an Appendix in the CPSRMS SSP to provide adequate traceability for decisions made prior to and after the implementation of CPSRMS.

3. Document the cost-benefit analysis for adding each of the supplemental NIST SP 800-53 controls. Additional explanatory details should added be to the CPSRMS SSP to justify the

additional 10 controls.

4. Include control parameters to the control descriptions in the SSP, where applicable.

5. Draft an implementation plan for each of the CPSRMS security controls, as well as for the four "Planned" controls identified without a planned implementation strategy (PM-10, SI-10, AU-9, and IA-8). The CPSRMS SSP should document the planned implementation strategy. This may be accomplished by updating the SCIP to include all controls identified in the CPSRMS SSP and CPSRMS SAR as "Other than Satisfied," "Planned," "Partially Compliant," or "Noncompliant."

6. All controls that were considered "Other than Satisfied," "Planned," "Partially Compliant," or "Noncompliant" as per the SSP or SAR should be included on the Plan of Actions and Milestones (POAM) or have the justification for their exclusion from the POAM documented.

Management Response: Management partially concurred with the finding, but indicated that the finding was based on the preliminary documents developed by CRI, which were developed in parallel with the development of the system and therefore contained inaccurate and incomplete information. Management indicated that since the OIG performed their fieldwork, substantial improvements had been made.

After the official launch of CPSRMS, the CPSRMS and IR staff performed an extensive internal assessment of the system and did a total rewrite of all documentation including the CPSRMS SSP and including updated system architecture, business functions, system interfaces, risk assessment, security categorization, security controls implementation, and security controls assessment.

Furthermore, it was determined that CPSRMS consisted of three subsystems: Public Portal, Business Portal, and CPS 360 (internal portal) and that each subsystem required an independent assessment of the security controls. The current version of the CPSRMS SSP contains independent assessments of the security controls for each subsystem.

The current version of the CPSRMS SSP was updated to be compliant with NIST (SP) 800-53 rev3 and NIST (SP) 800-53A rev1.

Specifically, in reference to recommendation number one of this finding, Management indicated that this type of security control definition would be most appropriately applied during the Requirements Phase of the System Integration Development Lifecycle (SDLC). Because the security controls were not initially included with the CPSRMS SDLC, this level of security definition was not possible. However, this level of security control description would be good for future phases of the project if security could be sufficiently integrated within the SDLC.

For recommendation number two, Management indicated the 10 additional controls referenced by the OIG had been removed from the CPSRMS SSP and therefore a cost benefit analysis for those controls was no longer necessary.

For recommendation number three, Management indicated that the information in question had been improved in the latest version of the CPSRMS SSP. Scoping, parameterization, and compensating controls are now described where needed in many of the controls.

For recommendation number four, Management indicated the planned controls are now documented in the NIST (SP) 800-53 section of the CPSRMS SSP; and that for new implementations, a SCIP would be developed and include all planned security controls.

For recommendation number five, Management indicated that controls had been updated with the latest internal assessment and Plan of Action and Milestones (POAM).

FINDING 4: The CPSRMS SSP did not reflect the most current information and often contradicted other Security control documents.

At the time of fieldwork, the CPSRMS SSP did not reflect the most current information and often contradicted other Security control documents. The disagreements and inconsistencies amongst the security control documents were attributable to management's inability to establish a methodology to reconcile the differences between the reporting styles of the two vendors who performed and documented the assessments. For example, each vendor used different criteria to define "Common," "Hybrid" and "System Specific" controls, as well as different criteria to assess compliance with the required NIST controls. Management did not know of the differences in criteria until being asked about them by the OIG. These inconsistencies in definitions and other areas led to an incomplete/inaccurate representation of the CPSRMS security profile and a general lack of consistency between the security control documents. For example, we noted the following:

a) The CPSRMS SSP stated that the CPSRMS "will be operational in October 2010" and the launch at the time of fieldwork was set for March 11, 2011.

b) Twenty devices identified in the CPSRMS system boundary as part of the SecureIT Inventory Assessment were not included in the CPSRMS SSP.

c) The CPSRMS SSP did not include the vulnerabilities identified as part of the Security Assessment Report and other technical assessments (*e.g.*, assessments performed by Aspect Security)

d) The CPSRMS SSP, developed by CRI, did not define "Common" controls the same way as the CPSRMS SAR developed by Secure IT or the GSS LAN. There are 17 System Specific/Hybrid controls assessed and defined in the SSP by SecureIT, as part of their independent validation of the implementation of NIST SP 800-53 security controls, and documented in the CPSRMS SAR as "System Specific" or "Hybrid" controls. These same controls were defined as "Common" when they were tested and documented as part of the GSS LAN SAR.

e) SecureIT's original assessment of SC-14 was "Not Compliant," which was documented (although never subsequently updated after its reassessment) in the GSS LAN SSP. When, after some remediation, SC-14 was reassessed as part of the CPSRMS SAR process it was deemed "In Place". However, CRI holds a different position and considers this control to be "Partially Compliant," as is documented in the CPSRMS SSP, even after the control reassessment. At the time of fieldwork, management had not documented which position it supported and their justification for holding this position.

f) Three controls: SI-03, SC-02, and SC-23, which were identified in the SAR as "Satisfied" were identified in the SCIP, either as "Planned," or "Solution Identified" but not implemented. Moreover, the CPSRMS SSP identified these three controls as either "Noncompliant" (SI -03) or "Partially Compliant" (SC-02 and SC-23).

Recommendations:

1. Update the SSP to include the correct go-live date and to reflect the latest understanding of the current state of CPSRMS security. As such, management should:

    a. Reconcile the CPSRMS SSP with the other security control documents (*e.g.*, CPSRMS SAR, GSS LAN SAR, SCIP, Security Categorization Document, and Risk Assessments), to identify all variances and update the documents to present one consistent "snapshot" of system security.

    b. Management should also perform an assessment to determine which position it supports regarding SC-14 (with significant weight given to the independent assessors) and justify/document their position in the SSP so that the SSP can be the single, authoritative security document for CPSRMS.

    c. Additionally, to support the objective of the CPSRMS SSP becoming the single, authoritative security document for CPSRMS, updates to the SSP should include the results of the related SARs and other technical security reviews (*e.g.*, Aspect Security reviews).

    d. Reassess the "Common," "Hybrid," and "System Specific" control significations, and update the SSP to include an accurate description of controls in addition to the justification for each of the control significations.

    e. The network should be re-scanned to define all of the devices within the CPSRMS System Boundary and the results of this scan should be included in the SSP. Moreover, management should reassess any additional controls required because of the discoveries made by this scan for proper implementation and document the results of this assessment in the SSP, if applicable.

2. A description of how CPSRMS is integrated into the Enterprise Architecture, which should include the Information Security Architecture, should be documented in the CPSRMS SSP.

3. Update the POAM to reflect the changes made to the updated SSP, where applicable.

Management Response: Management generally concurred with this finding, and provided the following update:

In reference to recommendation one, all of this work has been performed as part of the internal assessment and rewrite of the CPSRMS SSP. Version 2.4 of the CPSRMS SSP is now the single authoritative document.

In reference to recommendation three, the POAM has been updated in the latest versions of the SSP and POAM tracking database.

FINDING 5: The CPSRMS POAM does not include all elements required by OMB Memoranda 04-25.

At the time of fieldwork, the POAM did not include all OMB M-4-25 required components. It was noted that the CPSC's POAM process was in an immature state; resulting in incomplete implementation of the POAM. With incomplete implementation of the POAM, vulnerabilities may not be properly tracked and reported, leading to a lack of effective and timely remediation of the known issues. We noted that the following required components had been omitted from the POAM:

- milestone change records and related documentation to justify the changes;
- estimated resources used for the remediation effort and the related justification;
- justification for scheduling estimates and;
- estimated cost with its related justification and the funding source.

Additionally, the POAM included a field to define specific tasks and milestones; however, this field was not being utilized. Therefore, the specific tasks set forth to accomplish a particular remediation were not documented. Furthermore, the only dates that were defined in the POAM were the start, due, and completion dates for the issue as a whole; thus, the POAM did not define due dates for individual milestones.

Recommendation:

Update the POAM to include the missing information.

Management Response: Management concurred with the finding and noted that the latest version of the POAM has been updated in accordance with the audit's finding. The latest version of the CPSRMS POAM tracking database is available on the agency's SharePoint site.

FINDING 6: The CPSRMS Security Categorization Document does not adequately justify impact assignments for 10 of the identified information types.

At the time of fieldwork, the Categorization Document did not adequately justify the impact assignments for 10 of the identified information types, as required by NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*, dated August 2008. For example, the OIG found that the "Corrective Action" information type was categorized as "Low" in terms of "Availability." However, the assignment of this signification was justified in the text of the report using the same logic that was used to raise the "Population Health Management and Consumer Safety" information type from "Low" to "Moderate." These discrepancies appear to have been caused due to the agency not adequately documenting the justification it used for the impact assignments for the identified information types. Thus, there is a possibility that the impact assignments are inaccurate, causing an inaccuracy in the solution's overall impact rating. If the overall impact rating is inaccurate, the amount of effort to protect the solution may not be commensurate with the risk posed by the solution to the agency assets and mission.

In addition, it was noted the Categorization document states: "*Further analysis of data gathered as part of the development of the conceptual architecture and discussions with CPSC is required to establish special factors to raise or lower the impact levels of the security objectives*"; and no additional work had been performed as of the time fieldwork was conducted.

Please see table below for details surrounding each of the discrepancies.

Information Type Category	Language in Categorization Document	Impact Assigned in the Categorization Document	Appropriate NIST SP 800-60 Impact Assessment based on this language
Corrective Action	Confidentiality: Manufacturers and consumers will provide corrective actions for the various products. The protection of confidentiality for this information type has a low impact on CPSC, unless the consumer does not want to be identified.	Low	Moderate
Corrective Action	Availability: Much like the Population Health Management and Consumer Safety Information Type, users will expect this information to be available 24/7. This is a unique situation where the impact on the CPSC could be severe if the information is not available in a timely manner.	Low	High
Congressional Liaison	Confidentiality: This information may not be made available to the public	Low	Moderate

	unless of a public relations information type. If this is CPSC/congressional information, then this information will have a serious impact if confidentiality is compromised. If this was a reporting of public record then this information would be made available to the public and have a low impact.		
Congressional Liaison	Integrity: The integrity of this information will be important, regardless of whether it is disclosed publicly or remains internal to the CPSC. The impact of a compromise of integrity would have a serious impact.	Low	Moderate
Legal Prosecution and Litigation	Confidentiality: The Office of the General Counsel oversees Legal Prosecution and Litigation Type information and may disclose only a portion of the information to the public. The unauthorized disclosure of this information would have a serious impact on the CPSC and require protection.	Low	Moderate
Legal Prosecution and Litigation	Integrity: The integrity of this information, that is the unauthorized modification of legal prosecution and litigation information would also have a serious adverse impact on the CPSC and impede the case management system processes.	Low	Moderate
General Purpose Data and Statistics	Integrity: The integrity of this information is very important because it is used to perform statistical analysis and is used for decision support analysis. The impact of the unauthorized change or modification of this data would have a serious impact on the CPSC.	Low	Moderate
General Purpose Data and Statistics	Availability: Because this information primarily would be used during business hours, the availability of this data would be important and have a serious impact on the CPSC from 6 a.m.–8 p.m.; but if large statistical analyses are run overnight, the data may be required to be available 24/7.	Low	Moderate

Intellectual Property Protection	Integrity: The integrity of this information must be protected, especially if it is used for litigation purposes. The compromise of integrity for this information type could have a serious impact on the CPSC.	Low	Moderate
Population Health Management and Consumer Safety	Integrity: The compromise of the integrity of this information type could have a serious impact on the CPSC, a manufacturer, and a manufacturer's public image if the information is not correct. It is critical that this information is accurate.	Low	Moderate

Recommendation:

Perform an assessment to ensure adequate categorization of Information Types and that the logic for categorizing the Information Types as "High," "Moderate," or "Low" is consistent with the guidance provided in NIST SP 800-60.

Management Response: Management did concur with this finding as of the time of fieldwork; however, they noted that the finding is currently outdated, as the assessment recommended has now been performed. The latest version of the CPSRMS SSP version 2.4, includes an Appendix A dedicated to Security Categorization and justification for impact assignments. CPSRMS management and stakeholders selected the six information types used.

FINDING 7: Insufficient documentation of the analysis disqualifying the non-selected information types in the CPSRMS Security Categorization Document.

At the time of fieldwork, the Categorization Document contained justification of the selected information types that were chosen; however, the documentation of the analysis disqualifying the non-selected information types was omitted. Moreover, the Categorization document stated: "*At this point in the system lifecycle, it is still unclear whether the identified information types are appropriate and part of the CPSC vision for CPSRMS and its concept of operations.*" At the time of fieldwork, the referenced additional work had not been performed. This occurred due to a lack of management oversight of the CRI contract and to management not effectively enforcing the stipulations set forth in the CRI Statement of Work. The CPSRMS solution was assigned a "provisional" system impact rating based on the assessment of each of the selected information types documented in the Categorization document. Therefore, any missing or incomplete information in the assessment of these information types, although unlikely, may lead to an inaccurate system impact rating and consequently, which in turn may lead to the inaccurate selection of the security controls required by NIST SP 800-53.

Recommendation: Perform an analysis, as the Categorization document suggests, ensuring that all of the Information Types outlined in the NIST SP 800-60 framework were appropriately included or excluded. Include documentation of this analysis in the Categorization

documentation, along with the justification for including and excluding each of the Information Types chosen. Moreover, this analysis should be tied to the Enterprise Architecture. Additionally, CPSRMS's overall Security Impact assignment should be formalized once this NIST SP 800-60 assessment is completed.

Management Response: Management agreed that this recommendation was valid as of the time of fieldwork but noted that the finding is currently outdated, as remediation has been performed. Management indicated that the CPSRMS SSP version 2.4 includes an Appendix A that describes the security categorization process including the justification of the six information types that were selected by the stakeholders.

Additionally, management indicated that the analysis required for disqualifying the non-selected information types had not been performed and would not be performed. Management calculated that to analyze and document the justification for not selecting the remaining 224 information types would take approximately 112 hours or 14 days at an average of 30 minutes per information type. Management determined that the time needed to justify the non-selected information types could be used for more critical functions.

FINDING 8: The CPSRMS SSP does not outline the specific Public Access controls in place to mitigate the risks associated with allowing external user's access to CPSRMS.

At the time of fieldwork, the CPSRMS SSP did not outline specific Public Access controls in place to mitigate the risks associated with allowing external user's access to CPSRMS. OMB A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, dated November 28, 2000 states that, ". . . where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records." The CPSC's lack of compliance with this guidance is attributable to a lack of management oversight of the CRI contract, and to management not effectively enforcing the stipulations set forth in the CRI Statement of Work. Consequently, without effective controls in place governing Public Access, a public facing information system may provide an entry point for malicious users to the system in an unintended manner (ex. intentionally damage the system or obtain access to sensitive data). Moreover, this lack of control may also allow well-meaning users to inadvertently damage the system or access sensitive information.

Recommendation:

Define the specific Public Access controls in place/planned, or reference the document defining these controls within the CPSRMS SSP.

Management Response: Management did concur with this finding at the time of fieldwork; however, they noted that the finding is currently outdated. Management indicated that the CPSRMS SSP version 2.4, describes the NIST (SP) 800-53 security controls implementation to protect public access including Access and Account Management controls (passwords, session controls, account lockout, and eCaptcha) and Cryptographic Controls (SSLv3/TLS).

Consumer Product Safety Improvement Act of 2008
Section 212 Statutory Compliance Audit

This audit covered the CPSC's implementation of the publically available consumer product safety information database, and it assessed the database's compliance with Section 212 of the CPSIA. Overall, it was found that at the time of fieldwork, the CPSC has substantially complied with the requirements of the CPSIA for the database. However, one instance was noted in which personal information regarding a consumer (name, contact, and medical information) had been made available to the public. The type of information in question is characterized by the government as Personally Identifiable Information (PII), and its actual or potential unauthorized release is referred to as a breach of PII.

This particular breach of PII occurred because the CPSC did not properly conceal or redact the PII contained in a publically available Report of Harm. The breach in question was not discovered until a public user of the database notified the CPSC that a Report of Harm on the database contained an attachment that included the report submitter's name and phone number. The attachment also included a Web link to the report submitter's website, which included additional PII. The individual responsible for "scrubbing" the files to remove PII data before they were posted did not follow proper procedures. Instead, the individual attempted to redact the PII contained in the report by using Microsoft Word (the program that had also been used to generate the attachment) to add objects (black rectangles) to cover the PII information in the attachment. However, the objects were alterable by public users of the database, rendering the redaction meaningless and the information underneath viewable.

Recommendation: Upon notification of the PII breach, the CPSC acted to prevent similar situations from occurring in the future by restricting the database's public users from posting Microsoft Word (.doc and .docx file extensions) attachments to Reports of Harm. As such, all attachment submissions are now formatted in Adobe (.PDF file extension). This eliminated the ability of those charged with "scrubbing" PII from the files to add "objects" to attachments in an attempt to redact information submitted and it effectively forces them to follow proper procedures and make permanent redactions.

Management Response: Management concurred with our finding and immediately remediated the issue. Management has also instituted new procedures to prevent additional occurrences.

Office Relocations

Although a review of the agency's physical capital improvement efforts related to the relocation of offices at the CPSC HQ building was originally planned, this review has been canceled. An unpublished survey of relocation efforts was conducted as a precursor to the review and the preliminary results of this survey were shared with senior management. However, due to problems with the methodology of the survey, a number of its findings were deemed unreliable and its results could not be used to develop a formal review or audit.

Employee Complaints

No complaints fitting the definitions set forth in section 205(b) of the CPSIA have been filed with this office.

Christopher W. Dentel
Inspector General
U.S. Consumer Product Safety Commission

FISCAL YEAR 2012

Executive Summary

The Consumer Product Safety Improvement Act (CPSIA) of 2008 requires that the Office of Inspector General (OIG) of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the findings, conclusions, and recommendations from its reviews and audits performed under section 205 of the CPSIA. This year's report deals with the CPSC's capital improvement efforts involving information technology and the CPSC's laboratory accreditation program.

Capital Improvements: The CPSIA requires that the CPSC improve its information technology (IT) architecture in general, and that it establish and maintain a database on the safety of consumer products and other products or substances regulated by the Commission. The database must be publicly available, searchable, and accessible through the Internet website of the Commission. The development of this database will constitute, by a wide margin, the largest single IT project ever undertaken by the CPSC.

To meet these requirements, the CPSC has begun aggressively implementing a structured IT investment management process. This has proven to be particularly challenging because historically the CPSC dealt with the design and acquisition of its IT systems in an ad hoc manner. So in many ways, it had to start its implementation of a structured IT investment management process from scratch. To assess the CPSC's progress in this area, and to help provide the agency with guidance on how to continue to improve its processes, the CPSC OIG contracted with the public accounting firm of Withum, Smith+Brown (WS+B) to use the Information Technology Investment Maturity (ITIM) model developed by the Government Accountability Office (GAO) to audit the ITIM of the CPSC. WS+B found that the CPSC had taken several key steps in improving its ITIM processes, including the creation of an Investment Review Board and the adoption of its charter; the development of an IT investment portfolio; the formation of a Capital Planning and Investment Control Guide; the creation of a System Development Life Cycle Guide; and the implementation of IT Investment Classification Guidance. As a result of these and other activities, WS+B concluded that the CPSC had reached Stage 1 of the five-stage ITIM model, as defined by the GAO. In addition, WS+B found that the CPSC had implemented several of the key practices and critical processes that constitute Stage 2, but had yet to achieve that state. Based upon their assessment, WS+B provided a set of specific actions that the CPSC must accomplish to continue to improve its ITIM processes.

Laboratory Accreditation Program: The OIG's review of the CPSC's laboratory accreditation program focused on the program's internal controls. It found that although CPSC management had done a remarkable job of creating a laboratory accreditation program out of whole cloth at the time field work was being done, there were still areas of the program that needed improvement. In particular, perhaps because of the rate at which the program was created, written policies and procedures often were found to be lacking; aspects of the review process appeared to be subjective; and internal control design was deemed weak in certain areas of the program's management. The agency began taking aggressive measures to address several of these findings before the initial report was issued. Moreover, a number of these corrective measures have been implemented already; and it is anticipated that when this program is reviewed next year, the majority of this year's findings will have been addressed.

Introduction

This report has been prepared in accordance with the Consumer Product Safety Improvement Act (CPSIA) of 2008. The CPSIA constituted a comprehensive overhaul of consumer product safety rules, and it significantly impacted nearly all children's products entering the U.S. market.

The CPSIA also required that the Inspector General of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the Inspector General's findings, conclusions, and recommendations from the reviews and audits performed under subsections (a) and (b) of section 205 of the CPSIA. Those sections read as follows:

> **SEC. 205. INSPECTOR GENERAL AUDITS AND REPORTS.**
> (a) IMPROVEMENTS BY THE COMMISSION.—The Inspector General of the Commission shall conduct reviews and audits to assess—
>
> (1) the Commission's capital improvement efforts, including improvements and upgrades of the Commission's information technology architecture and systems and the development of the database of publicly available information on incidents involving injury or death required under section 6A of the Consumer Product Safety Act, as added by section 212 of this Act; and
>
> (2) the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by this Act, and overseeing the third party testing required by such section.
>
> (b) EMPLOYEE COMPLAINTS.—Within 1 year after the date of enactment of this Act, the Inspector General shall conduct a review of—
>
> (1) complaints received by the Inspector General from employees of the Commission about failures of other employees to enforce the rules or regulations of the Consumer Product Safety Act or any other Act enforced by the Commission or otherwise carry out their responsibilities under such Acts if such alleged failures raise issues of conflicts of interest, ethical violations, or the absence of good faith; and
>
> (2) actions taken by the Commission to address such failures and complaints, including an assessment of the timeliness and effectiveness of such actions.

This report fulfills the above-referenced requirements.

Assessment of Capital Improvement Efforts by the Commission

To meet this requirement in FY 2010, the CPSC OIG focused on the development of the database of publicly available information on incidents involving injury or death, required under section 6A of the Consumer Product Safety Act. Because this database is not operational yet—it is scheduled to be operational in spring 2011—it was impossible to assess its operational effectiveness.

However, a method was found to assess objectively the current status of the CPSC's efforts in this area, as well as provide the agency with a road map to meet the goals set out in the CPSIA. That method was the Government Accountability Office's (GAO) Information Technology Investment Maturity (ITIM) framework.

Background: The ITIM framework is a maturity model consisting of five progressive stages of maturity that allow an agency to achieve its ITIM capabilities. The maturity stages are cumulative; that is, in order to attain a higher stage of maturity, the agency must have institutionalized each of the requirements for that stage, in addition to those for each of the lower stages. The framework can be used to assess the maturity of an agency's investment management processes, leading to overall organizational improvement.

The GAO's ITIM maturity model framework offers organizations a guide for improving their IT investment management processes in a systematic and organized manner. These process improvements are intended to: increase the likelihood that investments will be completed on time, within budget, and with the expected functionality; promote better understanding and management of related risks; ensure that investments are selected based on their merits by a well-informed decision-making body; implement ideas and innovations to enhance process management; and increase the business value and mission performance of investments.

Under a contract monitored by the Office of Inspector General (OIG), Withum, Smith+Brown, PC (WS+B), an independent certified public accounting firm, performed an audit of the CPSC's ITIM processes, using the GAO's ITIM framework.[1]

Findings: WS+B found that the current condition of the CPSC's ITIM processes is primarily a function of the length of time that the CPSC has been working to fully develop and implement these processes. The passage of the Consumer Product Safety Improvement Act of 2008 (CPSIA) provided the impetus for the CPSC to upgrade its ITIM processes. Prior to that time, many of these processes were carried out in an *ad hoc* manner. To fund the public database project, the CPSC was required to submit an Exhibit 300,[2] to the OMB, which it submitted in

[1] The audit report, upon which this portion of the report is based, can be found at the CPSC OIG webpage at http://www.cpsc.gov/about/oig/oig.html.

[2] Exhibit 300 provides summary information and justification; summary of funding, acquisition and contract strategy; and earned value management, performance information, security, and enterprise architecture information related to capital investments.

September 2008. The CPSC has provided several updates on the database project to the OMB since then. As a result of the passage of the CPSIA, the CPSC received a mandate to:

- establish and maintain a database on the safety of consumer products that is publicly available, searchable, and accessible through the Internet;

- provide a detailed plan for establishing and maintaining the database, including plans for the operation, content, maintenance, and functionality of the database and details on the integration of the database into the Commission's overall information technology improvement objectives and plans; and

- expedite efforts to upgrade and improve the information technology systems in use by the Commission.

Since the passage of the CPSIA, the CPSC has been working to improve its ITIM practices. A year after passage of the CPSIA, the CPSC retained a capital planning manager from another federal agency, who is also serving as the Investment Review Board (IRB) chair. Because ITIM maturity stages are cumulative, where each stage is dependent upon completion of the previous stage, the CPSC has not been able to implement fully all of the Stage 2 critical processes and key practices.

As a result of these and other activities, WS+B concluded that the CPSC has reached Stage 1 of the five-stage ITIM model, as defined by the GAO. The CPSC has implemented several of the key practices and critical processes that constitute Stage 2. However, without adequate ITIM practices and procedures in place, the CPSC may not be able to reduce risk and heighten investment return; thus, the possibility exists that investments may not meet mission needs in the most cost-effective and efficient manner.

This takes on greater importance and urgency because the public database project is scheduled for implementation in spring 2011; currently, the launch of the public database is the most costly project in the CPSC's portfolio. The CPSC has performed additional activities and continues to develop and refine key practices following substantial completion of WS+B's assessments in July 2010.

Recommendations: WS+B determined that the following specific items need to be achieved for the CPSC to reach Stage 2 of ITIM maturity:

1. Ensure that the IRB has adequate resources, people, funding, and tools to support its operations and that these resources are identified and dedicated. The CPSC should identify the resources required for the effective operation of the IRB and ensure that the same is made available for investment execution and management.

2. Ensure that IRB members understand the CPSC's ITIM policies and procedures, as well as tools and techniques. The CPSC should organize a formal orientation session for its IRB members in areas such as economic evaluation techniques, capital budgeting methods, performance measurement strategies, and risk management approaches. The CPSC should

provide training to the IRB on the Capital Planning and Investment Control Guide (CPIC), focusing on the policy and criteria for identification and selection of IT projects.

3. Implement project management procedures for all projects and systems, including a dedicated project management office (PMO) modeled after CPSRMS's; although the extent of management procedures can vary, depending on the classification of the project. CPSC staff should continue to use the PMO dashboard as a tool to provide oversight and monitoring functions to ensure that projects receive the required oversight based upon the investment size and classification.

4. Establish procedures to ensure that users participate in project management throughout an IT project's life cycle, as CPSRMS has done. WS+B recommend that the CPSC provide additional resources to form an integrated Program Team or designated liaison within the program area to facilitate understanding of business needs. Internal user signoffs should be documented formally to evidence participation of the user departments.

5. Facilitate and enforce use of the CPIC Guide and the selection process for IT investments, as defined in the CPIC Guide for all projects.

6. Develop procedures to ensure that funding decisions are aligned with selection decisions, and that the IRB's IT portfolio recommendations are integrated more closely in the CPSC's budget process.

7. Develop procedures to ensure that all IT investment expenditures and acquisitions are made within the ITIM framework.

8. Ensure that the CPSC's IT projects and systems, including those in steady-state (operations and maintenance), are identified and that the required documents are collected in accordance with the CPIC Guide (including expected cost and schedule milestones, measurable benefit and risk expectations) to support decisions. These documents should be made available on the CPSC portal and updated, as necessary.

9. Ensure that data on actual performance, utilizing dashboards (including cost, schedule, benefit and risk performance), is made available to the IRB and reviewed regularly.

10. For each underperforming IT project or system, ensure that appropriate actions are taken to correct or terminate the project or system, in accordance with defined criteria and the documented policies and procedures for IRB oversight.

11. Ensure that the IRB regularly tracks the implementation of corrective actions for each underperforming project until the actions are completed.

Due to the cumulative nature of the ITIM maturity framework, Stages 3, 4, and 5 cannot be achieved until all of the critical processes in Stage 2 have been achieved. Therefore, it would be premature to propose a road map for Stages 3, 4, and 5. GAO research has shown that agency

efforts to improve investment management capabilities should focus on implementing all lower-stage practices before addressing the higher-stage practices.

Conclusion: Although it is too early to tell how effective the public database will be when it becomes operational, the steps taken by CPSC management to improve its ITIM processes certainly constitute movement in a positive direction. In FY 2011, after the publicly available database becomes operational, CPSC OIG will conduct a review of the public database project's effectiveness in meeting the criteria set forth in the CPSIA. To ensure that the CPSC has the appropriate investment management processes in place for the implementation of the public database project, and to improve its IT investment management processes over its entire investment portfolio, the OIG has recommended that the Chairman of the CPSC direct the Chief Information Officer to develop a plan of action and milestones (POA&M) to include timeframes for the completion of the remaining Stage 2 processes, as well as the subsequent stages.

Assessment of the Third Party Laboratory Accreditation Program

To assess the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by the CPSIA, and to oversee the third party testing required by such section, this office conducted a review of the CPSC's Laboratory Accreditation Program.

Background: In relevant part, the CPSIA imposed a third-party testing requirement on all consumer products intended primarily for children 12 years of age or younger. Every manufacturer (including an importer) or private labeler of a children's product must have its product tested by an accredited independent testing laboratory and, based on the testing, must issue a certificate that the product meets all applicable Consumer Product Safety Commission (CPSC) requirements. The CPSIA gave the CPSC the authority to directly accredit third party conformity assessment bodies (hereafter referred to as "third party laboratories") to do the required testing of children's products or designate independent accrediting organizations to accredit the testing laboratories. The CPSC is required to maintain an up-to-date list of accredited laboratories on its website. The CPSC has authority to suspend or terminate a laboratory's accreditation, in appropriate circumstances, and is required to periodically assess whether laboratories should continue to be accredited. The third party testing and certification requirements for children's products are phased in on a rolling schedule. The statute requires the CPSC to issue laboratory accreditation regimes for a variety of different categories of children's products.

The OIG's review focused on two specific areas. First, it evaluated whether internal controls were designed adequately and executed properly in the management of the laboratory accreditation program. Second, it assessed the CPSC's compliance with the CPSIA in the operation of its conformity assessment program. This review was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) issued by the Government Accountability Office.

The CPSC determined quickly that it lacked the necessary infrastructure to directly accredit the testing laboratories. So, to leverage its available resources, the CPSC used an independent accrediting organization to accredit the testing laboratories. The requirements for CPSC recognition include the following: (1) that the laboratory be accredited by a laboratory accreditation body that is a signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA); (2) that the laboratory scope of accreditation include the test methods required by CPSC laws and regulations; and (3) that the laboratory apply to the CPSC for recognition and agree to fulfill the requirements of the CPSC program.

In implementing the CPSIA, in general, and the laboratory accreditation program, in particular, the CPSC faced challenges created not only by the requirement that it promulgate rules within mandatory timelines, but also by the complex scientific, technical, and procedural issues surrounding the rules. For example, the first in the series of rules dealing with laboratory accreditation (not a subject traditionally within the CPSC's jurisdiction) had to be promulgated within 30 days of the enactment of the CPSIA.

The CPSIA expanded the authority and the responsibilities of the CPSC. Prior to the passage of the CPSIA, the agency had never participated in the accreditation of laboratories, and had not been confronted with the daunting task of developing a program to accredit laboratories and overseeing their testing of certain consumer products. The CPSIA established an aggressive regulatory agenda and set deadlines to ensure that results were achieved in a timely fashion. The vigorous requirements of the CPSIA have had positive as well as negative effects on the agency. The CPSIA has spurred a greater degree of regulatory activity. Meanwhile, it established implementation deadlines requiring the CPSC to move at a pace that it has not always been able to achieve.

Summary of Findings: The OIG found that although the CPSC has done a remarkable job of creating a laboratory accreditation program out of whole cloth at a time when field work was ongoing, there were other areas of the program that needed improvement. In particular, perhaps because of the rate at which the program was created, written policies and procedures often were lacking; certain aspects of the review process appeared to be subjective; and internal controls design was weak in certain areas of the program's management. As noted in the CPSC's responses to these findings, the agency began taking aggressive measures to address a number of the findings detailed in the report, even before the report was issued. Summaries of the specific findings made in the OIG's report are set forth below. [3]

Finding 1. <u>No Published Methodology or Detailed Criteria Developed for Evaluation of Government Laboratories</u>

We found that there was neither a published methodology nor detailed criteria established for the evaluation of government laboratories. The criteria for evaluating third-party and firewalled laboratories were spelled out fairly clearly and made available to the public on the CPSC's website. However, no such criteria have been published for government-controlled laboratories,

[3] The report containing the results of the review upon which this portion of this report is based, as well as management's responses to same, may be found at the CPSC OIG webpage at http://www.cpsc.gov/about/oig/oig.html.

and it appeared that no such criteria existed, at least in a written form.[4, 5]

As a result of the apparent lack of criteria, the evaluation of government laboratories may appear subjective. This appearance of subjectivity could increase the chances that an unsuccessful applicant would challenge the agency's decision to deny accreditation.

Recommendation: Develop a baseline or minimum set of documents and requirements that government laboratories must meet to be accredited; continue to use the current multi-person panel to evaluate applications to reduce subjectivity.

Finding 2. No Policies or Procedures Developed to Audit Third Party Laboratories as Condition of Continuing Accreditation

The CPSIA requires that no later than 10 months after the date of enactment of the CPSIA, the CPSC, by regulation, should establish requirements for the periodic audit of third party laboratories, as a condition of the continuing accreditation of such bodies. This requirement was to be completed by June 2009.

The CPSC does not have written policies or procedures in place to audit third party laboratories. As a result, the CPSC has no way of verifying whether the third party laboratories that it has accredited previously currently are complying with the accreditation requirements.

Recommendation: The CPSC should develop and implement written policies and procedures for auditing third party laboratories.

Finding 3. Inadequate Monitoring of Certification Expiration Dates

In accordance with section 102(e)(1)(B) of the CPSIA, the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds such laboratory failed to comply with an applicable protocol, standard, or requirement established by the CPSC.

However, the CPSC does not have written procedures to monitor whether certifications have expired certifications or whether certificates are up for renewal. Instead, the CPSC conducts follow-up checks— which are not documented or recorded—on an *ad hoc* basis.

The lack of documented procedures for monitoring certificate expiration dates increases the risk that an unauthorized laboratory will continue to be recognized as an accredited laboratory by the CPSC.

Recommendation: The CPSC should develop and implement procedures for regularly monitoring certification/certificate renewals and detecting expired certifications and

[4] The CPSIA establishes the underlying criteria to be evaluated (e.g., the existence of "undue influence"), but not how that evaluation should take place (e.g., independent investigation, information provided by other federal agencies).

[5] Since the completion of field work, the agency has made improvements in this area, including developing a standard set of questions and requests for documentation that it uses for all governmental lab applicants.

maintain records of these reviews. Laboratories with expired certifications should be removed from the accredited laboratory list maintained electronically by the CPSC.

Finding 4. No Written Policies or Procedures Exist for Removing Third Party Laboratory's Certification.

The CPSIA contemplates two situations that may lead to the withdrawal of a third party laboratory's certification. First, in accordance with CPSIA, Section 102(e)(1)(A), the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds that a manufacturer, private labeler, or governmental entity has exerted undue influence on such conformity assessment body or otherwise interfered with or compromised the integrity of the testing process with respect to the certification of a children's product. Second, CPSIA, Section 102(e)(1)(B) states that the CPSC may withdraw its accreditation or its acceptance of the accreditation of a third party laboratory if the CPSC finds such laboratory failed to comply with an applicable protocol, standard, or requirement established by the CPSC.

The CPSC does not have written policies or procedures to address the requirements of CPSIA, Section 102(e)(1)(A) or (B).

As a result, its process of withdrawing accreditation is not standardized, leaving the agency subject to a claim in court that it acted in an arbitrary and capricious manner when it withdraws accreditation from a laboratory. It is unclear what policies and procedures the CPSC will implement to withdraw recognition or acceptance of a third party laboratory's accreditation.

Recommendation: The CPSC should develop and implement written policies and procedures for withdrawing a third party laboratory's certification.

Finding 5. No Written Policies or Procedures Exist for Reviewing Employee Training Records Contained in Firewalled Laboratory Accreditation Application Packages

In addition to the baseline accreditation requirements, firewalled laboratories must submit in English, copies of their training documents to the CPSC. These documents should demonstrate that the laboratory's employees have been trained to understand that they may notify the CPSC immediately and confidentially of any attempt by a manufacturer, private labeler, or other interested party to hide or exert undue influence over the third party laboratories' test results. This additional requirement applies to any third party laboratory in which a manufacturer or private labeler of a children's product to be tested by the third party laboratory, owns an interest of 10 percent or more in the laboratory in question.

No written policies or procedures exist on how to implement the above-described requirements. During field work, we observed that there was little standardization or uniformity in the evaluation process. As a result, there is a lack of consistent enforcement or implementation of application requirements. For example, not all application packages examined contained the actual signatures of the employees who allegedly attended the training. The lack of employees' signatures on the training attendance list increases the difficulty of establishing whether the listed attendees actually received the training in question.

Recommendation: Develop and implement written policies and procedures to describe what constitutes acceptable training documents and related minimum requirements for firewalled laboratory application packages.

Finding 6. CPSC Failed to Meet Number of Accreditation Timeline Requirements

The CPSIA and related regulations created a number of timeline requirements for the establishment of accreditation requirements. The accreditation requirements for baby bouncers, walkers, and jumpers were to be established not later than 210 days after enactment of the CPSIA, or March 12, 2009. All other current CPSC children's product safety rules were to be created not later than 10 months after enactment of the CPSIA, or June 14, 2009). The CPSIA also required the CPSC to establish, by regulation, requirements for the periodic audit of third party laboratories, as a condition of the continuing accreditation of such bodies. The periodic audit requirement was supposed to be met not later than 10 months after the date of enactment of the CPSIA, June 14, 2009.

The CPSC did not publish *Federal Register* notices of accreditation requirements for baby bouncers, walkers, and jumpers by March 2009, as required by the CPSIA timeline.

Of the five classes of children's products mentioned specifically in the CPSIA regulation, four of the classes successfully met the timeline requirements, and only one class (baby bouncers, walkers, and jumpers) did not post before the required timeline expired. The rule for infant walkers finally posted to the *Federal Register* in June 2010, 15 months after the CPSIA timeline required.

There does not appear to be a predominate reason for the agency's failure to meet certain required timelines set forth in the CPSIA. In the case of baby bouncers, walkers, and jumpers, staff indicated the desire to produce a "better" rule than the previous rule. In the case of auditing third party laboratories, staff completed other projects demanding more immediate attention.

Recommendation: Increase the emphasis on meeting congressional mandates.

Finding 7. Overreliance on ILAC to Ensure Laboratories Conform to CPSIA Standards

At the time fieldwork was conducted, the CPSC was relying nearly exclusively on ILAC to ensure that the laboratories accredited by the CPSC actually conformed to CPSIA standards.

Although the CPSIA (Section 102(a)(1)(3)(C)) does permit the CPSC to accredit third party laboratories directly or through an independent accreditation organization, concerns exist about whether the CPSC demonstrated adequately and documented completely— prior to the agency opting for ILAC as the independent accreditation organization—that ILAC standards/test methods conform to CPSIA standards.

Based upon our findings, it appears that the CPSC may be relying too heavily on ILAC's accreditation process to determine whether to accredit laboratories as CPSIA compliant. It appears that tight deadlines and other resource constraints may be contributing factors in the CPSC's reliance on ILAC accreditation.

Recommendation: Consider conducting field visits or onsite inspections or employing some other monitoring mechanism to verify the validity and quality standards of third party laboratories. Perform these visits randomly, or when concerns arise, to limit reliance on ILAC certification.

Conclusion: Prior to the release of our original review, the CPSC already had undertaken aggressive measures to address our findings and recommendations. These included formal rulemaking—a rule is being developed that would address third party conformity assessment body requirements, including suspension and withdrawal of accreditation, as well as the development of internal agency procedures for overseeing accreditation. For example, the agency has developed a standard set of questions and requests for documentation to use for all governmental lab accreditation applicants. These standard requests are being published. Requests for information from U.S. missions abroad now also have a standard form. Thus, all applicants are reviewed using a standardized review document that provides the grounds for the agency's findings regarding the five criteria for governmental laboratories set forth in the statute. All relevant staff are being trained in these new procedures. In FY 2011, the OIG anticipates that a follow-up review will be completed to determine the effectiveness of these new policies and procedures.

Employee Complaints

No complaints fitting the definitions set forth in section 205(b) of the CPSIA have been filed with this office.

— S —

Christopher W. Dentel
Inspector General
U.S. Consumer Product Safety Commission

FISCAL YEAR 2013

Executive Summary

The Consumer Product Safety Improvement Act (CPSIA) of 2008 requires that the Office of Inspector General (OIG) of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the findings, conclusions, and recommendations from its reviews and audits performed under section 205 of the CPSIA. This year's report deals with the CPSC's capital improvement efforts involving information technology and the CPSC's laboratory accreditation program.

Capital Improvements: The CPSIA requires that the CPSC improve its information technology (IT) architecture in general. Last year's report dealt extensively with the CPSC's efforts to implement a structured IT investment management process. That will again be a focus of next year's report as a contract has been awarded to conduct a follow-up review of the CPSC's IT investment management process. However, this year's report focuses on the agency's efforts over the past several years to ensure the security of the information stored in the CPSC's IT systems.

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. It also requires that the relevant Office of Inspector General (OIG) perform an annual assessment of the agency's compliance with FISMA. The most recent available FISMA evaluation found that, although much work remains, management has made substantial progress in implementing the FISMA requirements.[1]

Laboratory Accreditation Program Follow-Up Review: The CPSIA requires that the CPSC Office of Inspector General review the adequacy of procedures developed by the CPSC for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by this Act.

The review conducted during this reporting period is a follow-up of the original review conducted over the CPSC's Third Party Laboratory Accreditation Program. The OIG's original review of the CPSC's laboratory accreditation program focused on the program's internal controls. It found that although CPSC management had done a remarkable job of creating a laboratory accreditation program out of whole cloth at the time field work was being done, there were still areas of the program that needed improvement. In particular, perhaps because of the rate at which the program was created, written policies and procedures often were found to be lacking; aspects of the review process appeared to be subjective; and internal control design was deemed weak in certain areas of the program's management. The follow-up review performed found that the agency had taken aggressive measures to address these findings.

[1] The FY 13 FISMA evaluation is currently underway, but the resulting report will not be issued until FY 14.

Introduction

This report has been prepared in accordance with the Consumer Product Safety Improvement Act (CPSIA) of 2008. The CPSIA requires that the Inspector General of the U.S. Consumer Product Safety Commission (CPSC) include in an annual report to the appropriate congressional committees, the Inspector General's findings, conclusions, and recommendations from the reviews and audits performed under subsections (a) and (b) of section 205 of the CPSIA. Those sections read as follows:

> **SEC. 205. INSPECTOR GENERAL AUDITS AND REPORTS.**
> (a) IMPROVEMENTS BY THE COMMISSION.—The Inspector General of the Commission shall conduct reviews and audits to assess—
>
> (1) the Commission's capital improvement efforts, including improvements and upgrades of the Commission's information technology architecture and systems and the development of the database of publicly available information on incidents involving injury or death required under section 6A of the Consumer Product Safety Act, as added by section 212 of this Act; and
>
> (2) the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by this Act, and overseeing the third party testing required by such section.
>
> (b) EMPLOYEE COMPLAINTS.—Within 1 year after the date of enactment of this Act, the Inspector General shall conduct a review of—
>
> (1) complaints received by the Inspector General from employees of the Commission about failures of other employees to enforce the rules or regulations of the Consumer Product Safety Act or any other Act enforced by the Commission or otherwise carry out their responsibilities under such Acts if such alleged failures raise issues of conflicts of interest, ethical violations, or the absence of good faith; and
>
> (2) actions taken by the Commission to address such failures and complaints, including an assessment of the timeliness and effectiveness of such actions.

This report fulfills the above-referenced requirements.

Assessment of the CPSC's Information Security Management

The Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. It also requires that the relevant Office of Inspector General (OIG) perform an annual assessment of the agency's compliance with FISMA. Each year's FISMA evaluation both follows-up on the findings from the previous years and assesses the agency against any new standards developed. This year's FISMA evaluation found that, although much work remains, management has made substantial progress in implementing the FISMA requirements.[2] This evaluation was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) issued by the Government Accountability Office.

The general theme of the findings was a lack of quality system reporting, in addition to, a lack of auditable evidence documenting the control activities performed by the resources responsible for the reviewed processes. These deficiencies, at least in part, resulted from a lack of adequate and up-to-date policies and procedures. Also contributing to the deficiencies identified was the lack of resources dedicated to implementing and enforcing the agency's documented policies and procedures throughout the Fiscal Year. Although management has updated many of the agency's IT security policies and improved several of their procedures, many improvements are still required. In addition, management did not disseminate these policies to all of the individuals/offices identified as having key procedural responsibilities.

The agency's system monitoring and reporting capabilities have substantially improved since FY 10. Management implemented several new tools in FY 11, and implemented a new IPS (Intrusion Prevention System) in FY 12. Although management has not fully optimized these tools, the system reporting possible now is far greater that it was a year ago and management has shown a commitment to continuing to improve the agency's system reporting capabilities. Management has also assigned an IT Security Specialist to the operations team to assist in the implementation and optimization of these tools.

Management has developed remediation strategies to address the known vulnerabilities, with a priority placed on the highest risk issues. The CPSC is in the process of remediating these issues. However, the full mitigation of these risks will require a significant amount of additional effort. For example, although the agency has still not fully implemented an effective Incident Response program, the CPSC has taken steps to remediate this issue. These steps include the establishment of a Computer Security Incident Response Team (CSIRT) to manage incidents. Management has also begun drafting detailed Standard Operating Procedures covering the incident response process, and management has begun to optimize the agency tool set to allow for the automatic identification and correlation of incidents.

---

[2] The report containing the results of the review upon which this portion of this report is based, as well as management's responses to same, may be found at the CPSC OIG webpage at http://www.cpsc.gov/about/oig/oig.html.

Another example of a remediation activity undertaken by CPSC management to eliminate existing vulnerabilities and improve overall system security is the continued improvement of the Continuous Monitoring Process. Although management has not fully implemented the Continuous Monitoring Plan, the security team is now providing monthly reports to senior management outlining the known risks to agency IT resources. This process will continue to improve as management optimizes its current tool set and improves system reporting. An effective Continuous Monitoring Process, once implemented, will result in the remediation of several other vulnerabilities, simply due to the improvements required in system reporting to facilitate the Continuous Monitoring strategy. The improvement in system reporting, in addition to the resulting analysis made possible by the enhanced reporting, will allow management to identify, quantify, and remediate weaknesses in other processes (such as Remote Access governance, Identity Management, and Security Incident Reporting) much more efficiently and effectively than is currently possible. This, in addition to the harmonizing of processes required for reporting, will result in a significant improvement in the overall system security.

Summary of Findings:

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. 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, as a result the techniques and concerns that are normally addressed by security 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 the 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 system and its inherent risk.

Actions Taken: Management has made significant progress to address this issue, although gaps remain. Management is currently in the process of hiring an additional Information Systems Security Officer to assist with the oversight of IT security. The agency has also developed an SSP for each of the accredited major applications (CPSRMS and ITDSRAM) in addition to the GSS LAN. The agency contracted outside consultancies to perform independent security control assessments each year for the GSS LAN since NIST enacted the requirement in 2006, except for Fiscal Years 2006, 2009, and 2011. The agency has also developed and formalized, although not yet fully implemented, a policy and procedure for establishing a certification and accreditation process, which generally conforms to the required NIST Framework standards.

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

In order to meet the accreditation and certifications requirements outlined above, and to determine whether management correctly and effectively implemented the security controls identified for the GSS LAN in the SSP, during 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 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. Management accomplished this 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 POAMs 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 management had made changes in 2009 to help the agency address this shortcoming, the agency has not historically used a POAM as an affirmative management tool in addressing security weaknesses. Although it had historically done a good job of documenting known security weaknesses and prioritizing them, the agency had not used a POAM to either track or project the resources required or milestones necessary to address these weaknesses (as required by the OMB). As a result, the agency lacked historical data regarding its past efforts and failed to take advantage of a powerful planning tool in addressing current and future IT security challenges. Moreover, as of the conclusion of the FY 12 FISMA review, management still had not adequately implemented the POAM. Management did not document milestones and milestone dates for each of the known security weaknesses. Also, management did not reference the related capital investments for each of the security weaknesses identified in the POAM.

Our FY 09 review determined that the GSS LAN 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, management had not updated or adequately tested the Contingency Plan in 2009, 2010, or 2011. Due to changes to the agency operating environment since the drafting of this plan, management decided that a new Information System Continuity Plan was necessary. To address this issue, management contracted an outside consultancy, Evoke, in FY 11 to draft Information System Contingency Plans (ISCP) for the GSS LAN and selected applications. Although management did not perform a functional test, as NIST requires, management performed a tabletop test of the GSS LAN ISCP, and documented the after-actions plans of the ISCP in November 2011. Now that management has drafted the GSS LAN ISCP, the agency is planning to complete a Business

Impact Analysis, establish an alternative processing site, and develop a Continuity of Operations Plan (COOP).

In FY 10, the CPSC contracted an outside vendor to perform and document the annual GSS LAN Risk Assessment, Security Test and Evaluation (ST&E), and Security Assessment Report (SAR), as well as to develop the SSP and to define a Continuous Monitoring process. This allowed the CPSC to identify risks, define compensating controls and outline remediation actions. The agency extended this contract in 2011 and 2012, and increased its scope to include the CPSRMS application. CPSRMS and ITDSRAM both obtained their security accreditation based on an independent security review of NIST requirements. CPSRMS obtained its accreditation in FY 11, and management reauthorized its security accreditation on October 3, 2012. ITDSRAM obtained its accreditation in FY 11. However, in FY 12, management did not have the ITSRAM application independently assessed for compliance with NIST requirements and did not formally reauthorize its security accreditation.

Also in FY 10 the Certification and Accreditation (C&A) policy did not define objective, measurable criteria that management could use to justify the certification and accreditation, recertification and reaccreditation, or conversely, decertification of an in-scope system. As of the FY 12 review, management still had not updated the policy. Furthermore, although the C&A policy addressed a process to continuously track changes to information systems that may necessitate reassessment of control effectiveness as defined by SP 800-37, management has not implemented a process to perform the security impact analyses necessary to perform these tasks.

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 areas of personnel security, data integrity, and documentation, CPSC management was not able to develop security procedures that focused on security mechanisms that affect the daily operation of the Commission. OMB Circular A-130, Appendix III requires that sufficient operational controls for personnel security, data integrity, and documentation be in place. This condition may have been due to the 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 areas of personnel security, data integrity, and documentation in order to ensure efficient and effective management of the IT systems in support of the CPSC's mission.

Status at Time of Review: Significant progress has been made since 2001 to address this issue. The CPSC developed the Information System Security Plan (SSP) for the GSS LAN in 2002. Patriot, the contractor that developed the SSP, reported that in order for the CPSC to adequately implement and maintain the requirements of the SSP, 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 2003 SSP. The CPSC has since hired an information system security officer and, in FY 11, provided him with one staff member to implement and maintain the SSP requirements. Management is also in the process of hiring a second information system security officer to oversee IT security. Management contracted out the remaining responsibilities on an "as needed" basis. However, management continues to require additional internal resources to adequately implement and maintain the SSP requirements.

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") The CPSC has since formalized a Configuration Management Policy to govern this process. However, management had not fully implemented this policy, developed attendant procedures, or implemented configuration baselines for all agency hardware and software.

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

Status at Time of Review: CPSC acknowledges its need for continued improvement. The CPSC has met the following goals in its effort to improve its security technical controls: implementing a security awareness training program, implementing solutions to perform automated system auditing, implementing the monitoring of Internet usage, implementing an Intrusion Prevention System, implementing multi-factor authentication for most agency resources, implementing a solution to restrict access to client USB ports by non-encrypted flash drives, implementing periodic reviews of user with elevated network privileges, and implementing a tool which allows the agency to inventory all network user accounts.

Assessment of the Third Party Laboratory Accreditation Program

To assess the adequacy of procedures for accrediting conformity assessment bodies as authorized by section 14(a)(3) of the Consumer Product Safety Act (15 U.S.C. 2063(a)(3)), as amended by the CPSIA, and to oversee the third party testing required by such section, this office conducted a review of the CPSC's Laboratory Accreditation Program.

Background: In relevant part, the CPSIA imposed a third-party testing requirement on all consumer products intended primarily for children 12 years of age or younger. Every manufacturer (including an importer) or private labeler of a children's product must have its product tested by an accredited independent testing laboratory and, based on the testing, must issue a certificate that the product meets all applicable Consumer Product Safety Commission (CPSC) requirements. The CPSIA gave the CPSC the authority to directly accredit third party conformity assessment bodies (hereafter referred to as "third party laboratories") to do the required testing of children's products or designate independent accrediting organizations to accredit the testing laboratories. The CPSC is required to maintain an up-to-date list of accredited laboratories on its website. The CPSC has authority to suspend or terminate a laboratory's accreditation, in appropriate circumstances, and is required to periodically assess whether laboratories should continue to be accredited. The third party testing and certification requirements for children's products are phased in on a rolling schedule. The statute requires the CPSC to issue laboratory accreditation regimes for a variety of different categories of children's products.

The OIG's review focused on two specific areas. First, it evaluated whether internal controls were designed adequately and executed properly in the management of the laboratory accreditation program. Second, it assessed the CPSC's compliance with the CPSIA in the operation of its conformity assessment program. This review was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) issued by the Government Accountability Office.

The CPSC determined quickly that it lacked the necessary infrastructure to directly accredit the testing laboratories. So, to leverage its available resources, the CPSC used an independent accrediting organization to accredit the testing laboratories. The requirements for CPSC recognition include the following: (1) that the laboratory be accredited by a laboratory accreditation body that is a signatory to the International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA); (2) that the laboratory scope of accreditation include the test methods required by CPSC laws and regulations; and (3) that the laboratory apply to the CPSC for recognition and agree to fulfill the requirements of the CPSC program.

In implementing the CPSIA, in general, and the laboratory accreditation program, in particular, the CPSC faced challenges created not only by the requirement that it promulgate rules within mandatory timelines, but also by the complex scientific, technical, and procedural issues surrounding the rules. For example, the first in the series of rules dealing with laboratory accreditation (not a subject traditionally within the CPSC's jurisdiction) had to be promulgated within 30 days of the enactment of the CPSIA.

The CPSIA expanded the authority and the responsibilities of the CPSC. Prior to the passage of the CPSIA, the agency had never participated in the accreditation of laboratories, and had not been confronted with the daunting task of developing a program to accredit laboratories and overseeing their testing of certain consumer products. The CPSIA established an aggressive regulatory agenda and set deadlines to ensure that results were achieved in a timely fashion. The vigorous requirements of the CPSIA have had positive as well as negative effects on the agency. The CPSIA has spurred a greater degree of regulatory activity. Meanwhile, it established implementation deadlines requiring the CPSC to move at a pace that it has not always been able to achieve.

Summary of Findings: The OIG found that although the CPSC has done a remarkable job of creating a laboratory accreditation program out of whole cloth at a time when field work was ongoing, there were other areas of the program that needed improvement. Initially, perhaps because of the rate at which the program was created, written policies and procedures often were lacking; certain aspects of the review process appeared to be subjective; and internal controls design was weak in certain areas of the program's management. The follow-up review found that the agency had taken aggressive measures to address a number of the findings detailed in the original report. Summaries of the specific findings made in the OIG's report are set forth below.[3]

Initial Finding 1. <u>No Published Methodology or Detailed Criteria Developed for Evaluation of Government Laboratories</u>

We found that there was neither a published methodology nor detailed criteria established for the evaluation of government laboratories. The criteria for evaluating third-party and firewalled laboratories were spelled out fairly clearly and made available to the public on the CPSC's website. However, no such criteria have been published for government-controlled laboratories, and it appeared that no such criteria existed, at least in a written form.[4]

As a result of the apparent lack of criteria, the evaluation of government laboratories may appear subjective. This appearance of subjectivity could increase the chances that an unsuccessful applicant would challenge the agency's decision to deny accreditation.

Recommendation: Develop a baseline or minimum set of documents and requirements that government laboratories must meet to be accredited; continue to use the current multi-person panel to evaluate applications to reduce subjectivity.

Actions Taken by Management to Implement Recommendation: The CPSC has developed a standard set of questions and requests for documentation that it uses for all governmental lab

[3] The report containing the results of the review upon which this portion of this report is based, as well as management's responses to same, may be found at the CPSC OIG webpage at http://www.cpsc.gov/about/oig/oig.html.

[4] The CPSIA establishes the underlying criteria to be evaluated (e.g., the existence of "undue influence"), but not how that evaluation should take place (e.g., independent investigation, information provided by other federal agencies).