

U.S. CONSUMER PRODUCT SAFETY COMMISSION



OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT

REPORT

Issued: December 13, 2013



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Memorandum

Date: December 13, 2013

TO : Robert S. Adler, Acting Chairman
Marietta Robinson, Commissioner
Ann Marie Buerkle, Commissioner

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Federal Information Security Management Act (FISMA) Evaluation

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements, although much work remains. The CPSC's General Support System (GSS LAN) has completed the security accreditation process and retained an active security accreditation. In addition, the Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDS/RAM) application, and cpsc.gov completed independent security assessments.

The agency's system monitoring and reporting capabilities have improved substantially. The system reporting and monitoring now possible are far greater than system reporting and monitoring were in FY 2010, and management has shown a commitment to continuing to improve these capabilities.

Management has also substantially improved the incident response process. The agency's improved system reporting and monitoring capabilities, combined with the agency's improved incident handling process, has positioned management to be able to take proactive steps to address known and potential vulnerabilities.

Although much has been accomplished, a good deal of work remains. The OIG noted that management has not updated and approved the major applications' security documentation, nor has management accepted the risk associated with operating these applications in FY 2013. Additionally, management has not fully implemented the NIST SP 800-37 Risk Management Framework. Management has not accredited or explicitly authorized the operation of 88 of the 91 inventoried CPSC applications in accordance with OMB M 10-15.

This year's review included 64 findings (8 high-risk findings). The IT challenges currently facing the agency are particularly relevant as the agency continues to deal with the implementation of the Consumer Product Safety Improvement Act (CPSIA), in general, and with the CPSIA's impacts on the agency's IT operations, in specific.

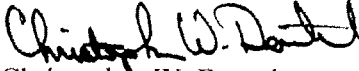
The general theme of the review's findings is a lack of CPSC resources dedicated to the implementation of security requirements.

Management continues to develop remediation strategies to address the known vulnerabilities, with a priority placed on the highest risk issues. However, the full mitigation of these risks will require a significant amount of additional effort. For example, management has not fully implemented Continuous Monitoring. Although management began providing monthly reports to senior management in FY 2012 outlining some of the known risks to agency IT resources, management did not update the agency's major applications' security documentation in FY 2013, or consistently provide senior management with the status of the agency's Plan of Actions and Milestones (POAMs) in FY 2013. Additionally, the monthly reports do not include a summary of the results of the improved system reporting and monitoring processes. The Continuous Monitoring process will only continue to improve if, as management optimizes its current tool set and improves system reporting, this information is shared with senior management.

In addition, management has not implemented Contingency Planning. Management has not developed a current Business Impact Analysis (BIA), and without a BIA, management cannot develop Business Contingency Plans, Disaster Recovery Plans, Information System Security Plans (ISCPs), or an agency Continuity of Operation Plan (COOP). Management has also not developed a workable Enterprise Architecture, which is critical in contingency planning and risk management.

Management (EXIT) has been briefed regarding the findings and recommendations of this audit and given an opportunity to respond to them. Management concurred with all of the findings and agreed to implement corrective actions regarding these findings. Management's responses concurring with the audit's findings are summarized at the end of the report.

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


Christopher W. Dentel
Inspector General

RESTRICTED

In Accordance With the Inspector Generals Act of 1974

Full or Partial Release of this document must be approved by the Office of the Inspector General and the Office of the General Counsel

Federal Information Security Management Act Report
Table of Contents

	Page
EXECUTIVE SUMMARY	2
Office of the Inspector General's Results	
INTRODUCTION	5
Background	5
Objective	6
Scope and Methodology	6
RESULTS OF EVALUATION	8
Prior Findings, Recommendations, and Actions Taken	
Security Management Controls	8
Security Operational Controls	24
Security Technical Controls	34
Management Response	44

FEDERAL INFORMATION MANAGEMENT ACT REPORT

EXECUTIVE SUMMARY

Office of the Inspector General's Results

To meet the requirements of the Government Information Security Reform Act (GISRA), and its successor, the Federal Information Security Management Act (FISMA), the Consumer Product Safety Commission's (CPSC) Office of the Inspector General (OIG) contracted with Grant Thornton, LLP, to perform an independent audit of the CPSC's automated information security control procedures and practices in fiscal year (FY) 2001. The audit included tests of entity-wide controls and six of the CPSC's 49 application systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology Special Publication (SP) 800XX, Draft Self-Assessment Guide for Information Technology Systems, March 9, 2001, to test security controls. The results of the Audit of Automated Information System Security, August 16, 2001, and the annual follow-ups to the audit, in conjunction with the independent reviews required by FISMA, and audits with information technology aspects (CFO Act Audit), served as the basis for the OIG's fiscal year 2013 evaluation. The OIG conducted this review 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) standards issued by the GAO.

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements, although much work remains. The CPSC's General Support System (GSS LAN) has completed the security accreditation process and retained an active security accreditation. In addition, the Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDS/RAM) application, and cpsc.gov completed independent security assessments.

The agency's system monitoring and reporting capabilities have improved substantially since FY 2010. Management implemented several new tools to achieve this end in FY 2011, FY 2012 and FY 2013. The system reporting and monitoring now possible are far greater than system reporting and monitoring were in FY 2010, and management has shown a commitment to continuing to improve these capabilities.

Management has substantially improved the incident response process. Management accomplished this by implementing a Cyber Security Incident Response Team (CSIRT), defining Standard Operating Procedures (SOPs), defining objective and reasonable metrics to assess the Incident Response Handling process, and implementing new solutions and improving existing solutions to facilitate the identification of security incidents. Additionally, although management does not consistently notify US-CERT in accordance with the timeframes outlined in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling, management began notifying US-CERT of security incidents in FY 2013. The agency's improved system reporting

and monitoring capabilities, combined with the agency's improved incident handling process, has positioned management to be able to take proactive steps to address known and potential vulnerabilities.

Although much has been accomplished, a good deal of work remains. The OIG noted that management has not updated and approved the major applications' security documentation, nor has management accepted the risk associated with operating these applications in FY 2013. Additionally, management has not fully implemented the NIST SP 800-37 Risk Management Framework. Management has not accredited or explicitly authorized the operation of 88 of the 91 inventoried CPSC applications in accordance with OMB M 10-15. The applications include, but are not limited to: Accellion, Budget, Concordance, Heat, Hotline, HSPD-12, Lab Accreditation, MaaS360, Microsoft Lync, PC-NEISS, Personnel, PRISM, FOIAExpress, Property Management System (PMS), Sample Tracking, WebAppSecurity, poolsafety.gov, recalls.gov, atvsafety.gov, cpsc.net, the EPI applications (EPDATA, EPHQ, EPID, EPIR, EPREVIEW, and EPQC) and Integrated Field System (IFS). Management also has not accredited the information resources at the laboratory site that reside outside of the GSS LAN security boundary. Management also has not performed an assessment to identify and categorize all major and minor agency applications. It is particularly important that management assess the EPI applications because of the applications' crucial importance to the agency mission and because of the potential of these applications to contain Personally Identifiable Information (PII). The OIG also noted 64 findings (8 high-risk findings) in this year's review; please see additional details below. The IT challenges currently facing the agency are particularly relevant as the agency continues to deal with the implementation of the Consumer Product Safety Improvement Act (CPSIA), in general, and with the CPSIA's impacts on the agency's IT operations, in specific.

The general theme of the review's findings is a lack of CPSC resources dedicated to the implementation of security requirements. Additionally, auditable evidence documenting the control activities performed by the resources responsible for the reviewed processes is lacking. These deficiencies, at least in part, resulted from a lack of adequate and up-to-date policies and procedures. In addition, as indicated earlier, the lack of resources dedicated to implementing and enforcing the agency's documented policies and procedures throughout the fiscal year contributes to the deficiencies identified. In FY 2013, management took steps to remediate these deficiencies. These steps included reassigning an existing Office of Information and Technology Services (EXIT) resource to the security operations staff and hiring an outside resource to assist with security policy and planning tasks. However, the new security policy and planning resource departed the agency after only three months, and management has not refilled the position.

Management continues to develop 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, management has not fully implemented Continuous Monitoring. Although management began providing monthly reports to senior management in FY 2012 outlining some of the known risks to agency IT resources, management did not update the agency's major applications' security documentation in FY 2013, or consistently provide senior management with the status of the agency's Plan of Actions and Milestones (POAMs) in

FY 2013. Additionally, the monthly reports do not include a summary of the results of the improved system reporting and monitoring processes. The Continuous Monitoring process will only continue to improve if, as management optimizes its current tool set and improves system reporting, this information is shared with senior management.

In addition, management has not implemented Contingency Planning. Management has not developed a current Business Impact Analysis (BIA), and without a BIA, management cannot develop Business Contingency Plans, Disaster Recovery Plans, Information System Security Plans (ISCPs), or an agency Continuity of Operation Plan (COOP). Management has also not developed a workable Enterprise Architecture, which is critical in contingency planning and risk management.

Management provided oral comments and concurs with the findings, conclusions, and recommendations described in the report. Auditors have worked closely with the responsible officials throughout the work and the parties are familiar with the findings and issues-addressed in the report. Management has not noted any disagreements with the findings, conclusions, and recommendations in the report, or major controversies with regard to the issues discussed in the report.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT REPORT

INTRODUCTION

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

To establish a baseline to help it meet the requirements outlined above, the CPSC's Office of the Inspector General (OIG) performed an independent review of the CPSC's automated information security control procedures and practices in FY 2013. The requirements of the review included:

- evaluating and testing the internal controls defined in the 2013 FISMA metrics (provided by DHS);
- testing the effectiveness of the information security controls defined in the 2013 FISMA metrics on all the CPSC's accredited, or previously accredited systems;
- assessing whether the CPSC's information security policies, procedures, and practices comply with the federal laws, regulations, and policies outlined in the 2013 FISMA metrics;
- recommending improvements, where necessary, in security record keeping, internal security controls, and system security;
- identifying the degree of risk associated with identified internal security controls weaknesses;

The review included tests of the entity-wide, system specific, and hybrid controls for the GSS LAN, cpsc.gov, CPSRMS, and International Trade Data System Risk Assessment Methodology (ITDSRAM) systems, as defined in the 2013 FISMA metrics. The OIG used the NIST and OMB guidance referred to in the 2013 FISMA metrics to assess the design and effectiveness of the CPSC security controls. The objective of the review was to determine whether the CPSC's automated information system was adequately safeguarded.

In its report, the OIG identified security weaknesses in the CPSC's management, operational, and technical controls policies, procedures, and practices. The conditions of these controls could permit the modification or destruction of data, disclosure of sensitive information, or denial of services to users who require the information to support the mission of the CPSC.

To ensure proper coverage and mitigation of the risks identified by the DHS, the CPSC is required to perform its own testing procedures to assess the design and implementation of the DHS defined FISMA requirements. The CPSC OIG reviewed the 2013 GSS LAN, CPSRMS, ITDSRAM, and cpsc.gov Security Assessment Plans (SAPs) and Security Assessment Reports (SARs), as well as the 2013 GSS LAN SSP. Management did not update the SSPs for the agency major applications in FY 2013. Therefore, the OIG could not review these documents. Also, important to note, the Office of Communications (OCM) became the cpsc.gov system owner during FY 2013 and now has full responsibility of cpsc.gov, including system security. The OIG assessment assessed all systems using the same methodology, irrespective of system ownership.

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

Scope and Methodology: The OIG conducted this evaluation from August to October of 2013. This evaluation consisted of a review of the following defined agency processes within the boundaries of the GSS LAN, CPSRMS, ITDSRAM and cpsc.gov systems:

- Risk Management
- Configuration Management
- Incident Response and Reporting
- Security Training
- The Plan of Actions and Milestones (POAM)
- Remote Access Management
- Identity and Access Management
- Continuous Monitoring Management
- Contingency Planning
- Contractor Systems
- Security Capital Planning

This evaluation constitutes both a follow-up of the findings and recommendations resulting from earlier audits, and a review of the CPSC's implementation of the IT security criteria as currently defined by FISMA. However, this year's evaluation does not consider the status of the CPSC Data Privacy Program, as current DHS guidance again this year does not require this reporting by the OIG.

The statuses of each of these topics were reviewed and discussed with the Chief Information Officer, Director of Information Technology and Technical Services, Information Systems Security Officer, and relevant members of their staffs. Documentation developed by both the CPSC officials and contractor personnel was reviewed as necessary.

The OIG conducted this evaluation 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 GAGAS standards issued by the GAO.

RESULTS OF EVALUATION

Prior Findings, Recommendations and Actions Taken: The FY 2001 audit of the CPSC's information security program revealed several material weaknesses in the CPSC's security policies, procedures, and practices. Specifically, CPSC management had not implemented sufficient management, operational, and technical controls. All previously identified material weaknesses have now been corrected. However, due to a combination of budget limitations and the new security system requirements promulgated by NIST and OMB, the CPSC failed to accomplish all of the new security requirements by their implementation target dates. All recommendations are considered open until all of the underlying weaknesses have been corrected. A summary of Prior Findings, Recommendations, and Actions Taken follows:

1. Security Management Controls

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

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

Actions Taken: Management has made significant progress since 2001 to address this issue, although gaps remain. Management hired an Information System Security Officer (ISSO) to oversee IT security. Management developed a System Development Lifecycle (SDLC) plan and a Business Continuity Plan (BCP) in FY 2003. Management also developed an Information System Security Plan (SSP) for the CPSC's General Support System (GSS LAN) in FY 2003. This adequately remediated all previous material weaknesses and allowed the GSS LAN to obtain a full Authorization to Operate (ATO) in FY 2004. Management hired another Information Systems Security Officer (ISSO) in FY 2013 to assist with the oversight of IT security. However, the new ISSO left the agency in July 2013, and management is in the process of refilling this position. The agency also developed an SSP for the following major applications (CPSRMS, ITDSRAM and cpsc.gov) 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 fully implemented, a policy and procedure for establishing a certification and accreditation process, which generally conforms to NIST Framework.

In FY 2005, in accordance with OMB guidance, the CPSC began using NIST SP 800-26 to perform agency security self-assessments and began implementing new system configuration policies. Efforts continue to this day to bring the CPSC into full compliance with all other FISMA and OMB requirements.

In FY 2006, new security system requirements previously promulgated by NIST and OMB became mandatory. 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 2006.

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 2007, 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 2008, 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 2009, 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 2013 FISMA review, management still had not adequately implemented POAMs to track or project resources required or milestones necessary to address all known security weaknesses. In addition, management did not reference the related capital investments for each of the security weaknesses identified in the agency POAMs.

Our FY 2009 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. Management also did not update or test the Contingency Plan in 2010, 2011 or 2013. Due to changes to the agency

operating environment since the initial 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 2011 to draft an Information System Contingency Plan (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 GSS LAN ISCP in November 2011. Management then certified the GSS LAN ISCP on March 2, 2012. In FY 2012, the vendors responsible for the implementation of the CPRMS and ITDSRAM applications also drafted ISCPs respectively. Management then assigned an internal resource to oversee agency Contingency Planning. However, this resource separated from the agency in FY 2013, and management is in the process of refilling this role. Management has not updated or tested the GSS LAN ISCP in FY 2013, and has not made any progress toward the completion of a Business Impact Analysis, the establishment of an alternative processing site, or the development of a Business Continuity Plan (BCP) or a Continuity of Operations Plan (COOP). In addition, management has not tested or certified the ITDSRAM or CPRMS ISCPs.

In FY 2010, the CPSC contracted an outside vendor to perform and document the annual GSS LAN Risk Assessment, Security Assessment Plan, 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 vendor performed these tasks for the GSS LAN again in FY 2013, and management reaccredited the GSS LAN again in FY 2013. The agency extended the vendor's contract in 2011, 2012 and increased its scope to include an independent review of the CPRMS application. In 2013, management increased this contract again to include the independent security control assessment of ITDSRAM, and cpsec.gov.

CPRMS, ITDSRAM, and cpsec.gov obtained their initial security accreditation based on an independent security review of NIST requirements and the completion of an SSP, Risk Assessment, and POAM. CPRMS obtained its accreditation in FY 2011, and management reauthorized its security accreditation on October 3, 2012. ITDSRAM obtained its accreditation in FY 2011. However, in FY 2012, management did not have the ITSRAM application independently assessed for compliance with NIST requirements and did not formally reauthorize its security accreditation. Cpsec.gov received its security authorization in FY 2012, and was independently assessed in FY 2013. However, in FY 2013, although management had CPRMS, ITDSRAM, and cpsec.gov's security controls independently reassessed and updated each of the agency SARs, management did not update any of the other relevant security documentation or reauthorize CPRMS, ITDSRAM, or cpsec.gov in FY 2013.

Additionally, in FY 2010 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 2013 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.

Risk Management Review:

Management has not developed an inventory of major applications and provided the inventory to the Agency Head for certification, as required by FISMA, section 3505(c)(2). Management has not inventoried or categorized the CPSC minor applications. Management has not selected, implemented, or assessed the security controls employed by the minor applications, or authorized the operation of the minor applications. Management has not assessed or accredited the mission-critical resources located at the lab that reside outside of the GSS LAN security boundary. These unaccredited resources reside on a separate network and do not take advantage of the network security controls and solutions provided by the GSS LAN. In addition, management has not designed and implemented additional security controls to mitigate the risk associated with these resources not taking advantage of the GSS LAN control solutions.

Management has not fully developed and implemented Risk Management Policies and procedures. The agency's policies and procedures do not include key elements related to the risk management process, and management has not reviewed/updated these policies and procedures in FY 2013. The current policies do not include how entities coordinate amongst themselves to perform critical risk management tasks (*e.g.*, how entities determine the risk to business processes or the organization as a whole). The current risk management process does not require agency officials to review and update these policies periodically; nor do those policies define how often the policies and procedures are to be reviewed and updated. Moreover, management has not codified the frequency with which management is required to disseminate the policies and procedures to resources with key responsibilities.

Furthermore, management has not fully implemented the C&A policies, and the C&A policies do not address the creation of the Risk Executive (function) role or another governing body required to provide oversight to the risk management process. Without these functions in place, and without their roles clearly defined and established, the organizational perspective of risk may be lost. Moreover, although the C&A policy requires the agency to create a Risk Management Strategy, and the policy outlines what is typically included in a Risk Management Strategy (the tools and procedures used to assess risk within the agency, how management prioritizes risks, how management monitors risk, and Organizational Risk Tolerance, etc.), this policy does not define what management must include in the agency's Risk Management Strategy or the procedures for developing that strategy. In fact, management has not developed a Risk Management Strategy.

Management has not developed and implemented an adequate process to define and accept risk when authorizing a system to operate. Management has not included guidance in any of the agency policies and procedures on how to define organizational risk tolerance or to ensure existing risks are within the organizational risk tolerance. Management has not developed an Enterprise Architecture (EA) or integrated EA into the agency's risk management process. Additionally, as mentioned previously, management has not developed an organization-wide risk management strategy. Without independent criteria, such as the organizational risk tolerance, an EA, and an organization-wide risk management strategy to provide guidance on what the

organization considers an acceptable risk, management cannot justify the decision to authorize a system to operate.

Management does not update security documents (SSPs, SARs, and Risk Assessments) throughout the year to provide an up-to-date view of the information systems' security posture and provide a method of continuously monitoring those postures, as required by NIST SP 800-37. Instead, as a matter of practice, management only updates these documents annually. Management did not develop periodic security status reports to document the assessment of control effectiveness and changes to the CPSRMS, ITDSRAM, and cpsc.gov systems and present these reports to the Authorizing Official, Risk Executive (function), and Information System owner, as required by NIST SP 800-37. In addition, management did not update the CPSRMS, ITDSRAM, or cpsc.gov risk assessments, SSPs, POAMs, annual security status reports, or reaccredit these systems in FY 2013, as required by the C&A policy and NIST SP 800-37.

Management did not include all of the OMB- and NIST-required information in the existing risk management documentation. For example, management did not adequately define the security authorization boundary in the GSS LAN security plan. Additionally, the documentation related to the annual independent assessment of agency security controls included several inconsistencies. The Security Assessment Plan documents the list of security controls the vendor agreed to assess. The Security Assessment Plan also includes the procedures the vendor agreed to use to assess the controls. However, the Security Assessment Reports, which describe the results of the assessment, do not reconcile with the approved Security Assessment Plans. Therefore, the independent assessor did not assess the agreed-upon controls or follow the agreed-upon procedures to assess the controls.

Risk Management Recommendations:

- 1) The agency should develop and implement standalone Risk Management policies and procedures, or, update and implement the C&A policy and ensure that the policy includes the following additional components:
 - a) Require management to implement a governance structure to manage risk from an organizational, mission, and solution level. [*e.g.*, the Risk Executive (function) and related governance bodies (Executive Risk Council)]. This policy should also include the roles and responsibilities for each resource involved with the governance of the risk management process.
 - b) Specify what management must include in the agency's Risk Management Strategy (*e.g.*, tools and procedures the agency uses to assess risk; the process by which management prioritizes risk; how management defines "organizational risk tolerance" and measures against that organizational risk tolerance; and how management plans to monitor risk throughout the year).
 - c) Explain the process by which management integrates the Enterprise Architecture into the risk management process.
 - d) Set forth the process by which decisions at the business process and solutions level are guided by the impact to the organization. This process should include the creation of an Executive Risk Council and the integration of EA into the risk management process.

e) Require management to base the authorization decision for an information system on the defined organizational risk tolerance.

f) Define the process by which the organizational entities coordinate with each other to address the requirements of the related policies and procedures.

g) Require the periodic review and update of information security policies and procedures.

h) Clarify the frequency with which the organization reviews/updates the policies and procedures.

i) Clarify the frequency with which the organization disseminates formal documented procedures to elements within the organization with associated roles and responsibilities.

j) Develop and disseminate a distribution list and requirement that management circulate the policies to all resources with key responsibilities outlined in the policies or procedures.

2) Management should develop and document a robust risk management process led by a Risk Executive (function). The Risk Executive (function) should report to a governing board that includes senior management. Management should also develop and implement a Risk Management Strategy using the NIST SP 800-37 guidance. The organization-wide Risk Management Strategy should include:

a) techniques and methodologies the organization plans to employ to assess information system related security risks and other types of risk of concern to the organization;

b) methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment;

c) the types and extent of risk mitigation measures the organization plans to employ to address identified risks;

d) the level of risk the organization plans to accept (*i.e.*, risk tolerance);

e) the methods and techniques the organization plans to use to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and

f) the degree and type of oversight the organization plans to use to ensure that management is effectively implementing the risk management strategy.

3) Management should document and certify a systems inventory that includes all CPSC systems and includes a description of each system in the systems inventory. The systems inventory description should include:

a) the interfaces with all other systems/networks,

b) the system criticality (based on a current BIA),

c) the security categorization (based on FIPS 199),

d) the hardware used by the system,

e) the databases used by the system,

f) the Authorization (ATO) status of each system, and

g) the name of the system owner.

4) The agency head should review the systems inventory annually, and whenever a major change occurs. Ultimately, this inventory should tie to the solutions architecture in the Enterprise Architecture.

- 5) Management should inventory and categorize each of the CPSC minor applications.
- 6) Management should select, implement, and assess the security controls employed by each of the CPSC minor applications. Management can include this information in the existing SSPs, where appropriate.
- 7) Management should formally authorize the operation of the minor applications once the minor applications' security controls are implemented.
- 8) Management should update all relevant security documentation (including SSPs, SARs, Risk Assessments, and POAMs) for the agency-defined major applications.
- 9) Management should provide the updated security documentation to the Authorizing Official to reauthorize the Major Applications to operate.
- 10) Management should update the GSS LAN SSP to include the accreditation boundary.
- 11) Management should perform and document Security Impact Analyses (SIAs) for system changes. The SIAs must include a sufficient level of detail to allow the CPSC security team to make a determination of the system change's impact on the agency's control environment.
- 12) Management should update all relevant security documentation (including baseline configuration documents, SSPs, SARs, Risk Assessments, and POAMs) each time a change with a security impact is made. Management should also update all relevant security documentation upon the completion of the annual security assessment. The agency should maintain SSPs as "living documents" to facilitate ongoing risk management decisions.
- 13) Monthly security status reports, developed to describe the results of the ongoing monitoring activities performed by the agency, should include the results of the Security Impact Analyses. At minimum, the security status reports should describe or summarize the results of the SIAs, key changes to SSPs, SARs, and POA&M's, and the results of the scans described in the Continuous Monitoring Plan.
- 14) Management should develop a comprehensive Enterprise Architecture (EA), and management should tie all system changes to the EA.
- 15) Management should provide training to resources responsible for implementing system and configuration changes. Management should train these resources on the CPSC change management procedures, and specify what information management requires when documenting a configuration change in a change management form.
- 16) Management should require that the vendor performing the independent security assessments include all security controls assessed, along with a description of the control implementations, in the agency SARs.

17) Management should develop and maintain an assessment schedule in an approved Continuous Monitoring Plan for all agency security controls and certify, justify, and document any changes to the assessment schedule.

18) Management should ensure that the independent assessor evaluate the controls based on the procedures outlined in the Security Assessment Plans.

19) Management should apply adequate security to the unaccredited resources located at the lab and accredit these resources in accordance with the relevant NIST and OMB guidance.

Management may accomplish this by:

a) reintegrating these resources back into the GSS LAN and ensuring compliance with all agency policies; or

b) designing and implementing security controls using a separate security function and structure to ensure that the lab network on which the resources run is in accordance with all applicable NIST and OMB guidance.

20) Management should include a summary of the agency's hardware and software inventory, noncompliance with all agency configuration baselines, missing patches, and all known server vulnerabilities in the monthly Security Status Reports.

POAM Review:

In FY 2010, management had not formalized or implemented the GSS LAN POAM, and management had not periodically notified program officials of the progress of the security issues identified in the GSS LAN POAM. Although gaps remain, the agency has formally implemented a POAM for the GSS LAN and has made improvements in this area. In FY 2011, management began documenting the identified security weaknesses and mapping those weaknesses to the source documents in a POAM. Management began documenting a scheduled completion date for each security weakness, assigning a remediation activity owner to each security weakness, documenting resources and timeline requirements for security weaknesses, and documenting some remediation milestones. Management also provided agency officials with quarterly updates on the changes to the GSS LAN POAM. However, management still does not consistently assign milestones and milestone dates to each security weakness or track changes to related milestones and milestone dates. Moreover, management still does not consistently document key milestones, the estimated resources, or the source of the funding required for remediating the security weaknesses. Management also still has not integrated the funding of the agency POAMs into the Capital Planning process. Management has documented requirements for recording agency POAMs in a policy document in FY 2011. However, management has not reviewed or updated the policy document since FY 2011.

In FY 2011, the CPSRMS and ITDSRAM applications both used POAMs to document and track material security weaknesses. However, management had not included all of the OMB M 04-25 required information in these POAMs. Management still does not document milestone completion dates or changes to milestones and milestone completion dates in the CPSRMS POAM. In addition, management still does not consistently include the following required information for each CPSRMS security weakness: the estimated funding resources required to

remediate the weakness, the remediation funding source, and key milestones. Additionally, the contractors and program officials responsible for implementing the CPSRMS solution did not provide an updated POAM for CPSRMS to the CIO on a quarterly basis throughout FY 2012; nor did program officials provide updates on the status of the CPSRMS POAM activities to the CIO on a quarterly basis. Although program officials did update the CPRMS POAM in Q2 and Q3, 2013, and program officials provided updates to the agency CIO on CPSRMS POAM activities at those times, program officials did not provide these updates consistently on a quarterly basis in FY 2013.

The ITDSRAM POAM also does not contain all of the OMB M 04-25-required information. The ITDSRAM POAM still does not document key milestones and the estimated completion dates for each of these milestones. The contractors and program officials responsible for implementing the ITDSRAM solution did not provide an updated POAM for ITDSRAM to the CIO on a quarterly basis throughout FY 2012 or in FY 2013; nor did they consistently provide updates on the status of the ITDSRAM POAM activities on a quarterly basis.

Late in FY 2012, management began using a POAM for the cpsc.gov solution to document and track material security weaknesses. However, management did not update the cpsc.gov POAM in FY 2013. Management also did not include all of the OMB M 04-25-required information in the cpsc.gov POAM. Management did not document the source (*e.g.*, program review, IG audit, and GAO audit) of the weakness identification, changes to the milestones and milestone dates, or the progress made in remediating each issue. In addition, management did not consistently document the following OMB M 04-25-required information in the cpsc.gov POAM for all of the documented security weaknesses: the key milestones, the completion dates associated with key milestones, the scheduled completion date for resolving the weakness, and the identity of the office or organization responsible for resolving the weakness.

Management does not adhere to the estimated completion dates for each of the weaknesses identified in the agency POAMs. Although management did not document estimated completion dates for POAM milestones, management did consistently document an estimated completion date for the resolution of the security weakness related to the GSS LAN, CPSRMS, and ITDSRAM. However, estimated completion dates documented in the GSS LAN POAM for 27 (90%) of the 30 open GSS LAN security weaknesses has passed. Additionally, at least one year has passed since the estimated completion date in 26 (96%) of the outstanding 27 security weaknesses documented on the GSS LAN POAM. The estimated completion date documented in the CPSRMS POAM has passed for 11 (48%) of the 23 open CPSRMS security weaknesses. Additionally, in each of the 29 instances where management documented an estimated completion date in the cpsc.gov POAM, the estimated completion date has passed. In all 29 instances, the security weaknesses have been outstanding for at least one year.

In FY 2011, the agency had not performed an annual security control assessment for the GSS LAN and CPSRMS, as required by NIST. Therefore, the agency did not document the security risks and vulnerabilities that management may have uncovered because of these assessments in the POAM. However, management had an independent assessment performed of the security controls for the GSS LAN and CPSRMS in FY 2012 and documented the security weaknesses identified as a result of these assessments in the associated POAMs. Management did not have

an independent assessment of security controls performed for the ITDSRAM application in FY 2012. Therefore, the FY 2012 ITDSRAM POAM did not include the results of an independent review. However, management did have an independent assessment performed for ITDSRAM in FY 2013; although these weaknesses did not appear in the ITDSRAM POAM. Due to the loss of the resource responsible for the maintenance of the Major Application's POAMs in the middle of the year, none of the Major Application's POAMs included the findings identified in the annual SARs.

POAM Recommendations:

- 1) Management should update the C&A policy to include a requirement to review and approve the policy on an annual basis or develop an entity level policy that requires all IT security policies and procedures to be reviewed and approved on an annual basis.
- 2) Management should perform a review of the C&A policy to ensure that the policy is current.
- 3) Management should disseminate the updated policy to all CPSC resources with a key role in the Risk Management, Certification and Accreditation and Plans of Action and Milestone processes.
- 4) Management should perform an assessment of the level of effort required for the remediation of each security weakness, and the results of that assessment should be reflected in the milestone/milestone dates and "Estimated Completion Date" fields in the associated POAMs.
- 5) Management should document the key milestones for all security weaknesses tracked on agency POAMs.
- 6) Management should document the dates associated with the key milestones for all security weaknesses tracked on the POAM.
- 7) Management should document all changes to the milestones or milestone dates in the POAM.
- 8) Security weaknesses documented in the POAM that are associated with investments identified in the IT Investment portfolio should include Unique Investment Identifiers (UIIs) to allow agency officials to trace the security weakness to the budget documentation.
- 9) Management should complete all POAM fields for all security weaknesses.
- 10) Management should capture milestones, milestone dates, and changes to milestone dates in the ITDSRAM POAM.
- 11) Management should document the source (*e.g.*, program review, IG audit, GAO audit, etc.) of the weakness identification, changes to the milestones and milestone dates, and the progress in remediating each security weakness in the cpsc.gov POAM.
- 12) Management should update the agency POAMs and maintain this information on the IT Security SharePoint.

13) Management should provide the updates to the CIO on all agency POAM activities on a quarterly basis.

14) Management should ensure that all findings identified in the agency SARs appear in the agency POAMs or provide justification for their exclusion.

Continuous Monitoring Review:

Management had an independent security control assessment of the GSS LAN performed in FY 2010 and documented the results in the SSP and SAR. However, management had not approved or implemented a Continuous Monitoring strategy. Additionally, documented policies and procedures for continuous monitoring did not and do not exist. Therefore, in FY 2011, management approved a Continuous Monitoring Plan developed by an outside vendor that included policy statements. Management also certified a Continuous Monitoring Plan that the outside vendor developed in FY 2012 that included CPSRMS. However, management has not approved the GSS LAN/CPSRMS Continuous Monitoring Plan drafted by the vendor in FY 2013. Additionally, management has not developed a Continuous Monitoring Plan for ITDSRAM or cpsc.gov.

Management should actively maintain agency SSPs, SARs, and POAMs to provide decision makers with an accurate representation of the system's current security posture at any given moment. However, management does not actively maintain the agency SSPs, SARs, and POAMs, and these documents do not act as the "living documents" that NIST SP 800-37 describes. In addition, management does not perform Security Impact Analyses (SIAs) on all proposed and actual system changes or update the security documentation with the results of these assessments.

Management has made progress in implementing the Continuous Monitoring program since FY 2010. For example, management presents monthly reports to program officials outlining current threats and the results of some of the agency's existing continuous monitoring activities. These reports include the results of periodic configuration compliance audits to identify FDCC/USGCB variances, as well as the results of periodic patch and vulnerability assessments. This process will continue to improve as management implements new monitoring tools and optimizes its existing tool set. However, management has not developed a comprehensive hardware/software inventory; management does not report all identified configuration variances or missing server/database patches; and management does not review logs to identify unauthorized access and privilege changes.

Continuous Monitoring Recommendations:

1) Management should implement the Risk Executive (function) and integrate that function into the Continuous Monitoring Process.

2) Management should develop, implement, and formalize OMB/NIST-compliant Continuous Monitoring Policies and attendant procedures.

- 3) Management should develop, implement, and formalize OMB/NIST-compliant Continuous Monitoring Plans for each of the agency systems.
- 4) Management should perform Security Impact Analyses (SIAs) on all actual or proposed system changes. Management should document these results, along with the results from all other continuous monitoring activities in the monthly Security Status Reports. Management should also update the risk documentation accordingly.
- 5) Management should develop and maintain a comprehensive Enterprise Architecture (EA), and management should tie the approval of all system changes to their impact on the EA.
- 6) Management should deploy a solution to report on the agency's current inventory of hardware and software.
- 7) The periodic security status reports should include the results of the server configuration management scans, patch management scans, and a summary of the current hardware and software inventory.
- 8) Management should ensure that quarterly configuration compliance audits are performed and that the results of these audits are presented to the ISSO. The results of these audits should be included in the relevant Monthly Security Status Reports.
- 9) Management should review logs and implement alerts to identify unauthorized access and privilege changes. The results of these reviews should be included in the Monthly Security Status Reports.
- 10) Management should regularly update agency security plans and POAMs, and the security plans and POAMs should act as "living documents" that represent the most up-to-date security information related to the CPSC systems.
- 11) Management should update all security documentation each time a major change occurs to a system, and management should use these documents in any decision to reaccredit the system or authorize the system to operate.
- 12) Management should draft annual Security Status Reports for the CPSRMS, ITDSRAM, and cpsc.gov applications and present these reports to the Authorizing Officials and System Owners for certification.

Contingency Planning Review:

The agency has not formalized a Business Impact Analysis (BIA), Business Continuity Plan (BCP), Disaster Recovery (DR) Plan, Continuity of Operations Plan (COOP), or Information System Contingency Plans (ISCP) for all agency systems. In FY 2012, management documented an ISCP for the GSS LAN, the cpsc.gov and CPSRMS applications, and performed a tabletop test on this ISCP. Management also drafted the continuity procedures in separate

ISCPs for ITDSRAM and CPSRMS applications. However, management has not adequately tested any of the ISCPs, as required by NIST SP 800-34; nor has management updated the ISCPs in FY 2013. Moreover, management has not defined Recovery Point Objectives (RPOs) for each of the critical systems, and management does not employ backup strategies to meet the RPOs documented in the ISCP.

Management finalized a Contingency Planning Policy in March 2012 and last updated the Contingency Planning Policy in September 2012. Our review of the Contingency Planning Policy found that the policy did not enumerate the test, training, and exercise (TT&E) program requirements required by FCDI. Additionally, management did not fully implement the Contingency Planning Policy. The agency had not performed and documented a Business Impact Analysis, developed or tested a Continuity of Operations Plan (COOP), Disaster Recovery (DR) Plan, Business Continuity Plan (BCP), or established an alternative processing site as required by NIST SP 800-34 and NIST SP 800-53. Management is looking into cloud technology to remediate these issues and expects to begin performing these tasks in 2015.

Contingency Planning Recommendations:

- 1) Management should enhance its Contingency Planning Policy and procedures to address all NIST and OMB requirements. EXIT management should solicit input from each of the CPSC departments when developing these policies and procedures to ensure proper coverage.
- 2) The CPSC should develop a standalone test, training, and exercise (TT&E) policy to govern the agency's TT&E program; alternatively the agency could enhance the existing Contingency Planning Policy to include TT&E requirements.
- 3) Management should train all of the relevant resources on the continuity planning responsibilities assigned to them in the policy.
- 4) Management should perform, document, and approve a formal Business Impact Analysis in accordance with NIST SP 800-34.
- 5) Management should develop, test, and approve an agency COOP in accordance with NIST SP 800-34.
- 6) Management should develop, test, and approve an agency DR Plan in accordance with NIST SP 800-34.
- 7) Management should develop, test, and approve an agency BCP in accordance with NIST SP 800-34.
- 8) Management should perform a functional test of the CPSC ISCPs in accordance with FEMA and NIST guidance.
- 9) Management should document the RPOs for all critical systems and implement a solution to allow management to meet these RPOs.

10) Management should draft after-action reports to document the “lessons learned” that are identified as part of the COOP, DR, and BCP plan testing.

11) Management should establish an alternative processing site. This site should contain the equipment and supplies required to resume operations in time to support the organization-defined time period for resumption.

Contractor Systems Review:

Management formalized a policy to govern the oversight of contractor systems and last updated/reviewed this policy on August 7, 2012. Management also developed a comprehensive inventory of third party systems that interconnect with agency systems in FY 2011, and management updated this inventory in FY 2012 and FY 2013. The CPSC uses Memorandums of Understanding (MOUs), Interconnect Security Agreements (ISAs), and Statements of Work (SOWs) to govern all inter-governmental IT relationships. However, in FY 2012, the CPSC began using cloud-based Software as a Service (SaaS) solution provided by a nongovernmental contractor, and the agency’s Contractor Security Oversight policies and procedures do not outline the process by which management controls such cloud-based Software as a Service (SaaS) implementation. Additionally, management did not develop or perform procedures to accredit any of the CPSC third party solutions, or to obtain assurance that the agency has implemented the user controls associated with those solutions.

Management has not established an information system connection or processing agreement with one contractor who has outside client machines connected to the agency network. Management also did not verify the implementation of the security controls specified in the CPSC information security policies and security plan for this contractor. Management plans to issue CPSC laptops to remediate this issue.

Management has not fully implemented the Contractor Security Oversight Policy. Management has not established processes and procedures to track the various interagency service agreements and their associated metrics. Management does not notify the contracted third parties of intrusions, attacks, or internal misuse so that the third party can take steps to determine whether its system has been compromised. Management does not analyze audit logs (by an automated tool or manual review) to detect and track unusual or suspicious activity across the interconnection that might indicate intrusions or internal misuse. Management does not use automated tools to scan for anomalies, unusual patterns, or known attack signatures and to alert administrators that the tools detected a threat. The ISSO or delegate does not periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize. Management does not coordinate contingency planning, training, testing, and exercises with any third party contractors to minimize the impact of disasters. In addition, management has not established joint procedures with the third parties based on existing contingency plans.

Contractor System Recommendations:

- 1) Management should update the Contractor Oversight Policies and Procedures to include the processes by which cloud-based Software as a Service implementation, such as Accellion, is controlled.
- 2) Management should establish processes and procedures to track the various interagency service agreements and metrics that management applies throughout the lifecycle of the contract.
- 3) Management should notify third parties of intrusions, attacks, or internal misuse so that the third party can take steps to determine whether the third party's system has been compromised.
- 4) Management should include a requirement in each ISA, requiring the connecting third parties to provide the CPSC with any known security weaknesses that might have an impact on the CPSC's mission.
- 5) Management should analyze audit logs to detect and track unusual or suspicious activity across the interconnections that might indicate intrusions or internal misuse.
- 6) Management should implement automated tools to scan for anomalies, unusual patterns, and known attack signatures; and management should configure these tools to alert administrators of detected threats.
- 7) The ISSO or delegate should periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize.
- 8) Management should coordinate contingency planning, training, testing, and exercises with the third party contractors to minimize the impact of disasters.
- 9) Management should establish joint procedures with the interconnecting third parties based on existing contingency plans.
- 10) Management should develop Security Plans for each of its third party solutions, have an independent assessment performed to ensure the design and effectiveness of the user controls documented in the Security Plan, and to accredit each of its third party solutions. FedRAMP outlines these user controls for the cloud-based solutions (Accellion). Management can also use the templates available on the FedRAMP site to help facilitate the control documentation process.
- 11) Management should accredit the systems used by the vendors connecting to the CPSC network who use non-CPSC machines. Management should develop a security plan and verify the implementation of required security controls on the external system, as specified in the organization's information security policy and security plan; and management should establish an approved information system connection or processing agreement with each of organizations hosting an external information system that connects to the agency network. Alternatively, management should provide the contractor with CPSC clients.

12) Management should update the Contractor Security Oversight policies/procedures to address explicitly what management must do to see that the agency adequately addresses all documented user-control considerations for each of the third party IT systems.

Security Capital Planning Review:

In FY 2011, management documented a process to govern the CPSC's Capital Planning, and Investment (CPIC) process that generally meets the requirements set forth in NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*. However, as of the OIG review in FY 2013, management had not fully implemented the above-described process. In addition, the policy and procedure documents in question do not meet all NIST SP 800-53 and OMB M 11-33 requirements. The procedures do not define how management plans and budgets for ongoing security costs, such as costs to perform the remediation activities outlined in the agency's POAMs. Additionally, management has not cross-referenced the agency POAMs to the Exhibits as required by OMB 11-33.

The OIG contracted Withum Smith+Brown (WS+B) to perform an Information Technology Investment Management (ITIM) assessment in August 2010, which included an audit of the CPIC process. At that time, WS+B reported that the agency's Investment Maturity Level was at stage one of the ITIM framework and only partially compliant with the stage two requirements. Although the OIG did not complete a reassessment of the agency Investment Maturity this fiscal year (this assessment is currently under way), management concedes that this assessment remains a work in progress, and management has not implemented all of the CPIC policies and procedures.

The agency uses contract services for the vast majority of its IT projects. The contractors, who are responsible for developing the systems in conjunction with the CPSC Security Team, are also responsible for implementing system security. Management allocates distinct line items for security costs in the organizational programming and documentation that tie to the Exhibits provided to the OMB in the fall. However, management does not allocate all security costs to each of the relevant individual investments.

The CPSC Investment Review Board (IRB) is responsible for prioritizing all facets of agency IT investments, including IT Security investments, against the agency mission. The consequent prioritization results in the decision to fund or withhold funding from a particular project for the next fiscal period. Furthermore, to ensure that management adequately prioritizes security in IT investments, the Information System Security Officer (ISSO) is a voting member of the weekly IT management prioritization meetings held by management, in part, to prepare investment recommendations for the IRB. Moreover, the ISSO participates in the IRB in a non-voting capacity.

Management also has assigned a separate project code for IT security within its time-keeping solution. This allows management to monitor the security efforts of its internal resources and account for those efforts better. Additionally, management is in the process of selecting a project management solution to mature this process. Once management implements a project

management solution, management will be in a better position to see that resources are available to perform the project tasks required.

Management also has not provided funding for the remediation of existing security weaknesses before implementing new projects as OMB requires. Management has funded several new projects in FY 2013, although security weaknesses exist that have been outstanding for years. If management does not remediate existing security weaknesses before implementing new projects, implementing a secure environment becomes increasingly more difficult.

Security Capital Planning Recommendations:

- 1) Management should update and implement existing agency Capital Planning and Investment Control policies and procedures, including the CPIC guide and the EA guide.
- 2) Management should enhance and implement existing policies/procedures to see that the costs associated with remediating security weaknesses are properly cross-referenced to the capital planning materials sent to OMB in the fall.
- 3) Management should enhance and implement existing policies/procedures to require agency personnel to document the appropriate investment's Unique Investment Identifier (UII) in each POAM. This will facilitate traceability from the agency's POAMs to its capital planning documentation.
- 4) Management should enhance and implement existing policies/procedures to require all POAMs to reflect the estimated resource needs for correcting reported weaknesses and to specify whether funds will come from a reallocation of base resources or a request for new funding. While the POAMs will not be used as agency funding requests by OMB, a brief rationale should be provided when a request for new funding is contemplated.
- 5) Management should develop and submit a Project Initiation Form for each outstanding security weakness identified on the agency POAMs requiring the initiation of a project with the IRB.
- 6) Management should document the Unique Investment Identifiers (UII) associated with each security weakness in the agency POAMs and record the cost to remediate the weakness in the appropriate investment. This is to link the security costs for a system to the security performance of a system.
- 7) Management should fund and remediate all existing POAMs before investing in new development projects.

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 unable to address security procedures to focus on security mechanisms that affect the daily operation of the Commission. OMB Circular A-130, Appendix III requires that sufficient operational controls for 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 for personnel security, data integrity, and documentation to foster efficient and effective management of the IT systems supporting the CPSC’s mission.

Action Taken: Significant progress has been made since 2001, to address this issue, even though gaps remain. As previously mentioned, the CPSC developed the Information System Security Plan (SSP) for the GSS LAN in 2002. Patriot, the contractor that developed the SSP, reported that for the CPSC to implement and maintain the requirements of the SSP adequately, a staff of three full-time personnel (information system security officer, network security engineer, and applications security engineer) is required. Qualifications for and responsibilities of each position were delineated in the 2003 SSP. The CPSC hired an Information System Security Officer (ISSO), and in FY 2011, CPSC provided him with one staff member to implement and maintain the SSP requirements. Management has since reassigned the ISSO’s staff member to perform operational security functions and hired a staff member to replace the reassigned staff member. However, the replacement staff member resigned after only three months, and management has not refilled the position yet. Management contracted out the remaining responsibilities on an “as needed” basis. However, management continues to require additional internal resources to implement and maintain adequately 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 has not fully implemented this policy, developed attendant procedures, or implemented configuration baselines for all agency hardware and software.

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

Configuration Management Review:

As a result of the OIG’s follow-up on actions taken to remediate prior findings, as well as the results of the FY 2010, FY 2011 and FY 2012 FISMA reviews, the OIG noted several

improvements and new findings. Although the agency baselined Windows XP in FY 2011, and implemented the United States Government Configuration Baseline (USGCB)-[formally, the Federal Desktop Core Configuration (FDCC)] recommended configurations for Windows XP, management did not properly document or implement baseline configurations for all other agency software or hardware components. In FY 2012 and FY 2013, management migrated to Windows 7 and IE8, and in the process, baselined the Windows 7 and IE8 images.

Management documented configuration baselines for the following software: Oracle, MySQL, Sybase, and SQL Server in FY 2011 and reviewed and updated these documented baselines in FY 2013. Management also documented the Windows 2008, SUSE Linux servers, Netware, VMWare, routers and switches in FY 2011. However, management has not reviewed or updated these baselines in FY 2012 or FY 2013. Additionally, management has not documented baseline configurations for any other system hardware or software, including the Windows Server 2003, Microsoft Lync, Microsoft Office, SharePoint Server 2007, Checkpoint firewall, and Cisco IOS. It is also important to note, management has not integrated updates to the baseline configuration documents into the change management process. Therefore, management does not capture in the baseline document (until the end of the year at the earliest) changes to systems and system environments that occur throughout the year. Management is reviewing a solution that will facilitate document change control.

In FY 2011, agency management began scanning agency clients for compliance with the required USGCB/FDCC settings, although management did not periodically scan IE8 for compliance in FY 2012 and FY 2013. In FY 2012, management began sharing a summary of these results in a monthly security status report. In addition, in FY 2012, management selected the Defense Information System Agency (DISA) settings, available in checklist form in the National Vulnerability Database (NVD), to apply to agency systems to harden them. Subsequently, management began scanning agency software for compliance with these checklists. Although management has not applied these settings to all agency systems, management began applying these settings to the Windows and Linux servers in FY 2012. Management has successfully applied these configurations to many more Windows and Linux servers in FY 2013. In September 2012, management began to perform non-credentialed scans of the network to identify vulnerabilities and continued to run these scans in FY 2013. However, the agency has still not developed and implemented a formal process to remediate the non-compliances identified in the USGCB/FDCC and DISA compliance scans or the vulnerabilities identified in the non-credentialed scans. Management also does not share the results of the DISA scans and the non-credentialed scans with all of the appropriate agency officials to ensure that they identify and eliminate similar vulnerabilities in other information systems (*i.e.*, systematic weaknesses).

Management has not developed and implemented Standard Operating Procedures (SOPs) for the Configuration Management process. Management does not maintain a comprehensive inventory of hardware and software. Therefore, management does not have a comprehensive inventory of critical hardware and software requiring configuration baselines. Management has not implemented the tools required to allow them to develop and maintain a comprehensive software/hardware inventory, and has not purged all known unauthorized software from the network. However, in FY 12, and continuing in FY 13, management improved its controls over

local administrator access to agency clients. Management limited the number of users with local administrative access to their clients and implemented a formal review of this access. With this improvement, management can ensure the agency only grants local administrator access to users requiring this access for their job functions. Although this improvement will not, in and of itself, remediate the issue, once management develops a comprehensive software inventory and implements a Virtual Desktop or whitelisting solution, the agency will have substantially better control over what software and hardware resides on its network. These improvements will also assist the agency with its efforts to improve property accountability and software license compliance. Management cannot achieve software license compliance without these tools and controls in place.

Management did not document all changes in the change control database or approve all documented changes before implementation in FY 2013. Management did not adequately document the testing procedures and results for each system change in FY 2013. Moreover, management does not adequately perform and document SIAs for each system change. The change control forms, which require completion before changes are implemented, do not provide enough information to make an accurate determination of how security will be affected because of the change. The resources performing and documenting the changes are not security experts. Because they are not experts, the resources are not qualified to complete the “How Security Affected” section in the change control form. Therefore, management cannot adequately perform an assessment to determine the security impact to the operating environment and control framework. Additionally, the ISSO did not approve all changes prior to implementation in FY 2012 or FY 2013.

The agency formalized a Change Management policy and Configuration Management Policy in FY 2011. However, it is missing key elements and management has not reviewed or updated the policy since FY 2011. Additionally, management has not fully implemented these policies. Management does not audit activities associated with system change control, and management did not document all changes/patches performed. Therefore, system administrators may implement unauthorized or inadequately tested changes on the production network, leaving the organization susceptible to unexpected system failures, as well as external and internal attacks.

The agency formalized a Patch Management policy in FY 2011. Although management did not review or update this policy in FY 2012, management did review and update the Patch Management policy in FY 2013. Management has not implemented an automated process to identify systematically on a monthly basis flaws or vulnerabilities for all CPSC servers or databases. Management also does not report server flaws and vulnerabilities in the Monthly Security Status Reports. However, management began performing monthly patch management scans of the Windows Server 2003, Windows 2008, and Linux servers in FY 2013. Management is considering options to begin scanning the ESX servers in the future.

Management has not documented a set of procedures for patching databases or third party applications, and management does not scan all databases periodically for missing patches and vulnerabilities. In addition, management does not implement client, server, database and widely-used application patches in a timely manner. Moreover, management is using versions of databases that are neither supported nor patched by their vendor.

Configuration Management Recommendations:

- 1) Management should review and update the Configuration Management policies and develop and implement SOPs to standardize the implementation of the Configuration Management process. The Configuration Management SOPs should include the following:
 - a) time frames in which the agency must remediate/accept identified baseline variances;
 - b) the process by which management documents and justifies baseline configurations deviations (including USGCB/FDCC and DISA deviations);
 - c) the process by which the agency reviews and updates the baseline configuration of each of the information systems, including how frequently the agency reviews and updates the baseline configurations, along with a list of agency-defined circumstances requiring the update of the baselines; the policy also should state how the agency updates to the baseline configurations as an integral part of information system component installations and upgrades;
 - d) the process by which the agency identifies and inventories hardware and software requiring configuration baselines;
 - e) the process by which the agency identifies and justifies all systems and system components not requiring baselines; currently, the policy refers to all “information systems.” However, management does not intend to baseline all information systems. Instead, the agency plans to determine the systems that require baselines and develop the configuration baselines accordingly.
 - f) what information management must include in each configuration baseline SOP.
- 2) The CPSC should develop an inventory of software and hardware requiring a configuration baseline, and management should document the process for developing this inventory in a procedure document. This should be done with the assistance of the business owners. Business owners should identify Mission Essential Functions and systems and provide this information to EXIT. Thereafter, EXIT should identify and inventory the software and hardware associated with these functions.
- 3) Management should develop and implement baseline configuration documents for all hardware and software components included in the inventory of software and hardware under configuration control, including, but not limited to, Windows Server 2003 and Microsoft Lync.
- 4) Management should review/update the existing configuration baselines each time a major change is made to the system’s environment, at least annually.
- 5) Management should patch all software identified in the software inventory.
- 6) The CPSC should establish and document mandatory configuration settings for information technology products employed within each information system, including, but not limited to,

Windows Server 2003 and Microsoft Lync. These configuration settings should use defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

- 7) Subsequently, management should implement the identified configuration settings.
- 8) Management should identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system, based on explicit operational requirements.
- 9) Thereafter, management should monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- 10) The agency should implement a solution to develop and maintain a current and comprehensive software/hardware inventory. Management can install agents on all CPSC machines to allow the agency to use Simple Network Management Protocol (SNMP) to develop a hardware inventory. However, this approach includes known security risks. Therefore, if management chooses to address this finding by implementing SNMP, then management should perform an assessment of the risks posed by SNMP.
- 11) Management should purge the network of all unauthorized software.
- 12) Management should implement a whitelisting or VDI solution to prevent systematically unauthorized software from running on the network.
- 13) On a monthly basis, management should scan IE8 to ensure compliance with FDCC/USGCB requirements and remediate any identified variances in compliance with a formally documented policy document.
- 14) Management should perform and document Security Impact Analyses for each system change. The Security Impact Analyses should include a sufficient level of detail to allow the CPSC security team to make a determination of a system change's impact to the agency's control environment.
- 15) Monthly security status reports, developed to describe the results of the ongoing continuous monitoring activities performed by the agency, should include the results of the Security Impact Analyses. At minimum, the security status reports should describe or summarize the results of the SIAs, key changes to SSPs, SARs, and POA&Ms, and the results of the scans described in the Continuous Monitoring Plan.
- 16) Management should develop a comprehensive Enterprise Architecture, and management should tie all system changes to the EA.
- 17) Management should actively maintain and update all baseline configuration documents. Management should update baseline configuration documents any time a change is implemented that has an impact on the baseline configurations.

- 18) Management should develop a process to remediate non-compliances with the baseline configurations identified as part of monthly scans and document that process in an SOP.
 - a) Management should include a requirement to document a remediation plan for all non-compliances identified as part of the monthly configuration management scans in the Configuration Management Policy (or related SOPs).
 - b) Management should document required timeframes for the remediation of non-compliances identified as part of the monthly configuration management scans in the Configuration Management Policy (or related SOPs).
- 19) Management should implement the process outlined in recommendation 18 above, and ensure that the agency remediates configuration baseline non-compliances in a timely manner.
- 20) Management should implement and document controls to mitigate the risk posed by the accepted variances to the configuration baselines.
- 21) Management should include the results of the patch management, configuration management (USGCB/DISA), and non-credentialed vulnerability scans in the monthly security status reports.
- 22) Management should provide detailed results from configuration management and vulnerability scans to each of the branch chiefs to allow for the identification of systematic weaknesses/deficiencies.
- 23) Management should update the baseline configuration documents, as appropriate, to reflect any changes resulting from the configuration changes and patches.
- 24) Management should audit production changes periodically to validate that the agency has adequately tested, documented, and approved the production changes.
- 25) The ISSO or delegate should approve all system changes.
- 26) Management should document all changes (including patches) in the change control database.
- 27) Management should provide training to resources responsible for implementing system and configuration changes. Management should train these resources on the CPSC change management procedures and identify what information management requires when documenting a configuration change in a change management form (*e.g.*, security impact, test cases, test methodologies, test results, etc...)
- 28) Management should develop an SOP outlining the database and third party application patch management process; and management should reference the database patching SOP in the Patch Management Policy.

- 29) Management should periodically scan the CPSC databases and third party applications for vulnerabilities and missing patches and remediate accordingly. If the agency decides not to implement the missing patch, management should document a formal justification.
- 30) Management should upgrade to a supported version of Oracle and Sybase, or migrate to another supported database.
- 31) Management should implement an automated process to identify flaws systematically and implement patches for all CPSC servers and databases.
- 32) Management should implement client, server, database, and widely used application patches in a timely manner and in accordance with the patch management policy.
- 33) Management should test all client, server, database, and application patches in a test environment prior to deploying the patch to production.
- 34) Management should document all client, server, database, and application patches in the change management database and document the process used to test these patches.
- 35) Management should add separate queries to the change management database to allow users to search on server, database, and application patches.
- 36) Management should improve the process for managing IT software requests. Management should implement an automated tool (such as SharePoint) that houses all of the IT software request information and software licensing information. Management should use this tool to obtain and document software requests. Management should also use this tool to systematically require approval by the appropriate resources prior to closing/completing the new software request.
- 37) Management should develop and enforce a process to govern software license compliance:
 - a) Management should document and maintain a comprehensive software inventory.
 - b) Management should document the number of instances of each type of software installed on the network.
 - c) Management should document and inventory all software licenses owned by the agency.
 - d) Management should reconcile the software instances installed on the network to the software licenses owned by the CPSC and remediate any discrepancies.
 - e) Management should perform periodic audits to ensure compliance.

Incident Response and Reporting review:

The agency developed and formalized an Incident Response Policy on August 20, 2011, and management last reviewed and updated the policy on July 25, 2013. Management implemented an Incident Reporting database, to track incident reports, and this tool resides on the IT Security SharePoint site. Management also maintains the existing Incident Response policy, procedures, and plan in the IT Security SharePoint site. However, management has not fully implemented the policy.

Management has assigned resources to a Computer Security Incident Response Team (CSIRT) in accordance with changes made to the Incident Response policy on January 28, 2013. The CSIRT has analyzed, validated, and documented all known security incidents since this policy change. However, management has not trained these resources on incident handling in accordance with the policy. Management also does not perform annual audits to ensure compliance with the Incident Response Policy, as required by the Incident Response Policy.

The CSIRT documents and tracks all known security incidents in security incident reports available in the Incident Response Database. The security incident reports include the date the incident began, a description of the incident, the priority of the incident, comments from incident handlers, the status of the incident, and the next steps to be taken. However, the OIG could not attest to the timeliness of the security team's response to and resolution of security incidents because management did not consistently document the time the CSIRT was notified of the security incident.

The agency implemented an Incident Response SOP in FY 2013, which outlined law enforcement notification requirements. However, no incidents requiring law enforcement notification occurred within FY 2013. Therefore, the OIG could not assess to determine whether management notified law enforcement in accordance with the timeframes outlined in the Incident Response Policy.

Additionally, management began notifying US-CERT of security incidents in FY 2013. However, management does not consistently notify CSIRT of lost or stolen laptops and Blackberries. Management also does not consistently document the time the CSIRT was notified of security incidents. Therefore, the CSIRT did not notify the United States Computer Response Readiness Team (US-CERT) in accordance with the timeframes outlined in the Incident Response Policy and in the Federal Guidelines.

Management implemented several solutions since FY 2011 to improve management's ability to monitor for incidents. Management has implemented the Trusted Internet Connection (TIC), a log management solution, and a solution to monitor outbound traffic. The TIC consolidates external network connections across the federal government. The TIC also allows for the central monitoring of network traffic for malicious activity, across the government. A monitoring tool called Einstein, which management implemented in conjunction with the TIC, facilitates this monitoring. The Einstein solution monitors for specific predefined signatures of known malicious activity at the agencies' Internet connections. Einstein alerts US-CERT directly when Einstein detects specific malicious network activity matching predetermined signatures, allowing the CPSC to use US-CERT expertise and resources.

Management implemented and configured a log management solution to notify system administrators of a list of predefined security events identified by other network monitoring solutions. Management has not yet fully optimized the log management solution; although management made significant progress in this effort in FY 2012 and FY 2013. For example, the log management solution now notifies management of the occurrence of predefined events across 10 different monitoring tools. In FY 2013, management implemented a solution to

monitor for actions constituting internal threats and to identify unauthorized activity by inspecting outbound network traffic.

Incident Response and Reporting Recommendations:

- 1) Management should provide formal training to the CSIRT members on the Incident Handling process, in accordance with the Incident Response Policy.
- 2) Management should perform an annual audit to assess compliance with the Incident Response Policy, in accordance with the Incident Response Policy.
- 3) Management should document the time and date the security team/CSIRT is first notified of the incident in the SharePoint tool used to monitor the incidents.
- 4) Management should not only date-stamp, but also time-stamp all actions taken to address security issues in the incident response reports.
- 5) Management should notify US-CERT and law enforcement of security incidents within the federally and organizationally prescribed timeframes.
- 6) Management should update the Property Management policies and SOPs to require Property Custodians to notify the ISSO/CSIRT of missing devices that may contain CPSC data (e.g., flash drives, external hard drives, desktops, servers, laptops, Blackberries, etc...) identified throughout the year (e.g., when notified of a lost/stolen device, or as identified as part of the inventory process).
- 7) Management should train all Property Custodians on their responsibility to notify the ISSO/CSIRT of lost or stolen devices that may contain CPSC data identified throughout the year.

Security Training:

Although management did not review or update the Security Training policies in FY 2013, only one element is missing from the CPSC's Security Awareness and Training policies and procedures. The Security Awareness and Training policies do not include the requirement for the agency to provide security training based on the 25 user groups outlined in NIST SP 800-16. The agency does not provide role-based training to its resources. Instead of developing individualized security training for each of the 25 specific user groups outlined in NIST SP 800-16, the agency provides one training course for all CPSC personnel and provides additional training courses for personnel within the IT department with significant information security responsibilities. However, although management customizes the training courses management provides to the IT security personnel, management did not provide training to address IT security from a System Development Lifecycle (SDLC) perspective, as required by NIST SP 800-16.

Management's increased efforts to ensure CPSC personnel complete the agency-provided security awareness training have resulted in substantial improvements. In FY 2012, management implemented a zero-tolerance approach to address personnel who do not complete their annual security awareness training. Management now revokes computer access to any user who does not complete the CPSC-provided security awareness training course within the prescribed timeframes. Implementing this approach has increased security awareness training participation from 67.5 percent in FY 2011 to 96 percent in FY 2012 and to 90percent in FY 2013.

Security Training Recommendations:

- 1) The agency should update the Security Training Policy and develop a NIST SP 800-16 compliant training program.
 - a) The Security Awareness and Training policies and procedures should require management to provide each NIST SP 800-16 "user group," defined within the agency security training program, role-based training specifically developed for their group.
 - b) The training criteria, if not the content, for each user group should be outlined in the policy. For details on the required training criteria, please see NIST SP 800-16, pages 98–154; NIST SP 800-16, appendix E; and summaries in NIST SP 800-50, pages 25–27.
- 2) Agency management should assign all agency resources to one of the 25 user groups documented in NIST SP 800-16.
- 3) Once assigned to a NIST SP 800-16-defined user group, agency management should then select appropriate training courses and provide security training to those agency resources commensurate with their user groups. The DHS Information System Security Line of Business (ISSLOB) has been working with agencies to develop a standardized curriculum and to select information security Shared Service Centers (SSC). The ISSLOB SSCs provide an efficient and cost-effective solution for agencies to procure general information security training for employees and contractors. For more information on this program, contact the ISSLOB program management office at: isslob@dhs.gov.

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, sensitive information was left vulnerable. This condition apparently stemmed from CPSC management lacking the resources to make implementation of sufficient technical controls a priority. The level of risk was rated high for identification and authentication and logical access.

Prior Recommendation: CPSC management should implement sufficient technical controls for identification and authentication, logical access, and audit trails to protect the information used to support the Commission's mission.

Action Taken: The effectiveness of six of the CPSC's systems, and the underlying elements of each, were tested during the FY 2001 audit. Weaknesses identified in controls related to these systems contributed to the overall condition of the CPSC's information security program. As reported in the management response to the original audit, the CPSC requested funding in fiscal years 1999 through 2002, without success, to establish a capital budget for information technology. The need for such funds was also included, unsuccessfully, in the CPSC's FY 2003 and FY 2004 budget requests. Budget requests cited the need for new investments to protect the current operating capability and efficiency of information technology. According to the Budget Officer, in the absence of a capital budget for information technology, the CPSC has applied some savings from operating funds to this area. In FY 2002, the CPSC dedicated more than \$500,000 from one-time salary savings to develop an SSP, address data system weaknesses, enhanced firewall intrusion detection capabilities, and other operating and system application enhancements. In FY 2003, the total CPSC Information Technology commitment was \$714,891 from salaries and other expenses. In FY 2004, the CPSC committed \$715,000 for its Information Technology programs. In FY 2005, this figure rose to \$1,035,100. In FY 2006, the CPSC spent \$2,082,050 on its IT programs. In FY 2007, the CPSC committed \$6,300,000 to its IT program. In FY 2008, the CPSC's commitment rose to 30 FTEs and \$13,000,000. In FY 2009, the CPSC's commitment rose to 31.1 FTEs and \$19,832,939. In FY 2010, the CPSC's commitment rose to \$26,492,137. However, in FY 2010, the number of FTEs fell to 30.9. In FY 2011, the CPSC's Information Technology commitment fell to \$23,617,310. However, FTEs increased from 30.9 in FY 2010 to 36.6 in FY 2011. In FY 2012, the CPSC's expenditures committed to IT services fell to \$21,617,065, and FTEs decreased to 36.4. In FY 2013, the CPSC's commitment to IT services fell to 19,192,869, and FTEs decreased to 32.5. Work on implementing the recommendations contained in the SSPs and more recent guidance continues.

The CPSC acknowledges the need for continued improvement. Over the past few years, the CPSC has met the following goals to improve the agency's security technical controls: implementing a security awareness training program, implementing solutions to perform automated system auditing, implementing solutions to monitor Internet usage, implementing an Intrusion Prevention System, implementing a Network Access Control solution, implementing multifactor authentication for most agency resources, implementing a solution to restrict access to client USB ports by non-encrypted flash drives, implementing periodic reviews of users with elevated network privileges, and implementing a tool that allows the agency to inventory all network user accounts.

Remote Access Management review:

Management developed and formalized policies for authorizing, monitoring, and controlling remote access in FY 2011, and management updated and recertified these policies in FY 2012. However, management did not update the Remote Access Management policies in FY 2013, and the Remote Access Policy refers to processes that have since changed. Additionally, the Remote Access Management policy does not include a list of security functions and security-related information that users can access remotely or the additional controls management has implemented to ensure that these users do not misuse this access. Additionally, management has not defined within the policies and procedures the networking protocols that the agency has deemed non-secure.

Although management has developed Teleworking and Remote Access procedures, these procedures do not address several operational topics. The procedures do not provide for checking for upgrades and patches to the remote access software components and acquiring, testing, and deploying those updates. The procedures do not address reconfiguring access control features, as needed, based on factors such as: policy changes, technology changes, audit findings, and new security needs. Moreover, the procedures do not address detecting and documenting anomalies identified within the remote access infrastructure. Such anomalies might indicate malicious activity or deviations from policies and procedures. These anomalies should be reported to other systems' administrators, as appropriate.

Procedures for system monitoring have improved substantially. Management has implemented controls, such as ingress filtering, egress filtering, and deep packet reviews. However, management has not fully implemented the remote access policies and procedures. Management does not monitor for unauthorized remote access connections or monitor authorized remote access connections for misuse. The agency also has a policy that requires users to encrypt all sensitive information before transmitting the information outside the internal network. However, although the agency implemented a tool to facilitate compliance with this requirement in FY 2012, management has not configured the CPSC e-mail solution to encrypt e-mails systematically before transmission across a public network. In addition, management does not perform audits to ensure that all sensitive e-mails and attachments transmitted across a public network use the encryption tool appropriately. Therefore, although the process has improved with the implementation of the encryption tool, an extremely high likelihood remains that users send unencrypted, sensitive files over public networks.

Management does not require all users to use multifactor authentication to access the network. Although management has not fully satisfied the NIST SP 800-53 requirements in this area, management has made substantial progress toward that goal, and only a limited number of users exist who can access the network without the use of their Personal Identification Verification (PIV) Card. Management does not uniquely identify and authenticate all users accessing the network. Management has not implemented a formal process to control the establishment and maintenance of common E-Directory and Active Directory (AD) accounts. Additionally, management does not change common account credentials when users separate from the agency or change job functions. Moreover, the Network Engineering and Computer Support Teams use generic administrator IDs to perform support functions. Agency resources that have administrative rights access the GSS LAN remotely, using administrator accounts. Furthermore, management does not monitor the tasks performed by the administrators while using these IDs.

Management does not properly document and report lost or stolen laptops/Blackberries. Management did not document all of the laptops and Blackberries lost in FY 2013 in the Incident Reporting database. Management also did not report all of these lost devices to US-CERT. This is due to users and Property Custodians not reporting lost or stolen laptops and Blackberries to the CSIRT/ISSO upon discovery. In addition, management does not document the time the user reports the lost/stolen device. Therefore, management cannot document the timeliness of its notification to US-CERT for these types of events. Furthermore, management could not provide evidence that four lost/stolen laptops identified in FY 2013 were encrypted.

Remote Access Management Recommendations:

- 1) Management should document and implement the following processes in a policy or procedure document:
 - a) A list of the security functions and security-related information that users can access remotely and the additional controls in place to ensure that these functions are not misused. In addition, management should implement and document specific audit procedures to ensure that these controls exist and work effectively.
 - b) An inventory of networking protocols management deems non-secure. Management should also implement a policy to ensure that access to these non-secure protocols is restricted.
 - c) A requirement for management to route all remote accesses through managed access points.
- 2) The agency should follow the documented Remote Access Policy and the NIST requirements by implementing automated tools to monitor for unauthorized remote access connections and to monitor for misuse of authorized remote access connections. Management should also report the results of these analyses to all appropriate parties.
- 3) Management should implement a solution to require systematically the encryption of all sensitive information transmitted across a public network. Alternatively, management should audit periodically e-mails and attachments traversing a public network to ensure policy compliance. Management could also implement a data loss prevention (DLP) solution.
- 4) Management should systematically require multifactor authentication for all users accessing the CPSC network.
- 5) Management should implement a formal process to approve the creation of new common user accounts.
- 6) Management should implement a formal process to establish membership in the common agency accounts.
- 7) Management should implement a formal process to disable common user accounts once these accounts are no longer required.
- 8) Management should implement a formal process to change the common user account's credentials once a member separates from the agency or changes job functions and no longer requires access to the account.
- 9) Management should require a formal periodic review of all common user accounts to ensure that these accounts remain appropriate.
- 10) Management should create separate non-administrative user accounts for administrators, and require administrators to use these accounts when performing tasks that do not require administrative privileges.

11) Management should grant administrators local administrative accounts to each CPSC server, individually, instead of using the global system administrator accounts. Management should check-in/check-out the passwords to the global system administrator accounts only when this access is required.

12) Management should implement a formal process to require management to change the credentials on shared administrator accounts whenever a user with knowledge of these credentials separates from the CPSC or changes job functions.

13) Management should require periodic password changes on all common accounts.

14) Management should enhance the existing automated encryption solution or implement another solution that reports on, and maintains historical records of, the encryption status of all devices containing CPSC data.

Identity and Access Management review:

The agency formalized the General Access Control policy on August 10, 2011, and last updated and recertified the policy on September 10, 2012. However, the procedures outlined in the General Access Control policy did not include several key elements. These procedures did not include: the process by which management establishes and controls common/shared network accounts; the process by which management establishes and controls temporary, emergency, and guest accounts; the process by which management establishes and controls system accounts; and account modification procedures. Management did not reference the individual system access control SOPs for the agency's major applications in the General Access Policy. Management also has not finalized an Access Control Policy and attendant procedures for CPSRMS, nor has management developed an Access Control Policy and attendant procedures for cpsc.gov.

Although management has a formalized General Access Control Policy, management has not fully implemented this policy. The General Access Control Policy requires that agency management audit all users with access to the CPSC systems and confirm the accuracy of the group access settings. Management is also required to submit the results of these audits to the ISSO for record and maintenance purposes. However, management does not perform this audit. In addition, although management began performing periodic user access reviews for many agency systems on a semiannual basis in FY 2012, management did not perform a periodic review of network accounts in FY 2013.

The CPSC GSS does not uniquely identify and authenticate all devices before establishing a connection to the CPSC GSS. The agency implemented a Network Access Control (NAC) solution in FY 2013 that it expects to remediate this issue when configured and reporting properly. However, management has not fully configured the NAC solution to perform all of the tasks required. In addition, with the NAC solution's current configuration, its reporting and alerting capabilities are not reliable.

Management does not require multifactor authentication for all users to access the CPSC network. However, management has made significant progress in implementing this requirement. Management has configured agency clients to allow multifactor authentication, and management plans to require agency clients systematically to use multifactor authentication in FY 2014. Once management implements the systematic requirement for multifactor authentication, only network administrators will be able to access the CPSC network without using multifactor authentication. Management has decided to accept the risk associated with this vulnerability.

The agency has not implemented the Principle of Least Privilege and proper separation of duties for the GSS LAN. The agency does not have the ability to report on users with access to specific security functions within AD or E-Directory. Because the agency has not implemented a solution that will allow them to develop reports with this level of granularity, management cannot apply the Principle of Least Privilege. Additionally, due to the limited number of resources dedicated to IT support and the broad range of IT functions supported, some of these functions are, by necessity, performed by the same individual. If a user has administrator access, the user can perform all security functions, even if their specific job function does not require this ability. This has prevented management from implementing the proper separation of duties. In addition, administrators have sufficient access to perform system administration and access and alter the audit logs. Furthermore, users with administrative rights have the ability to access the GSS remotely using their administrator accounts. Management does not require separate accounts for these users to telework or perform non-administrative tasks.

The agency has not implemented the Principle of Least Privilege for CPSRMS or cpsec.gov. All CPS360 (a CPSRMS subsystem) users can view all incident reports, even those that management has not approved for public consumption, whether or not their job function requires access to these data views. Additionally, management has not implemented roles within cpsec.gov or developed a workflow within cpsec.gov to require approval from management to publish content to the CPSC website. All users who have access to author content on cpsec.gov have sufficient access to publish without further adjudication.

Management began performing weekly staffing report reviews in FY 2012 to ensure that the agency revoked separating employees' access to the network in a timely manner; and management continued this practice in FY 2013. However, management does not perform this reconciliation for all agency systems. The OIG also noted that, even with the improvement to the process, management does not consistently disable access to the agency network accounts or other information system accounts immediately upon employee and contractor separation. The OIG identified separated employees and contractors whom management had not revoked from agency information systems as of September 30, 2013. In addition, management does not record the time and date that management disables all user accounts and cannot provide evidence of the timeliness of these revocations.

The OIG also noted management has not implemented an effective process for tracking and inventorying CPSC contractors. The contractor inventory and separation reports contain inaccuracies. For example, active contractors appear on the contractor separation reports. The contractor inventory process is a manual process that requires coordination between EXRM,

EXIT, and agency Contracting Officer's Representatives (CORs). Management has not developed and does not actively maintain a centralized contractor database to track contractor on-boarding and off-boarding. This, in addition to the lack of process standardization, has limited management's ability to revoke in a timely manner the information system access for separating contractors.

Identity and Access Management Recommendations:

- 1) Management should review and update the General Access Control policy annually.
- 2) Management should include the following elements in the General Access Control Policy and procedure documents:
 - a) roles and responsibilities and guidance on how management coordinates access control tasks between the CPSC branches.
 - b) the process by which management establishes and controls common network accounts; this should include how management authorizes and monitors common/anonymous accounts;
 - c) the process by which management establishes and controls temporary, emergency and guest accounts, including guidance on how management authorizes and monitors guest/temporary accounts; the procedures should define a process for notifying account managers when temporary accounts are no longer required and should also include a requirement to deactivate temporary accounts that management no longer requires;
 - d) the process by which the agency establishes and controls system accounts;
 - e) the procedures for the establishment and modification of user accounts, including a requirement for all new administrators to follow the formal user access request process; and
 - f) a requirement that the General Access Policy reference the individual system access control SOPs.
- 3) Management should draft, approve, and implement NIST-compliant Access Control policies and procedures for CPSRMS, ITDSRAM, and cpsc.gov.
- 4) Management should ensure that the General Access Control Policy is fully implemented. This includes requiring that:
 - a) the ITTS Branch Chiefs and program managers assess access controls for all users with administrative and non-administrative access privileges on an annual basis;
 - b) management maintains documentation to include a list of all security systems and security controls in place for each system;
 - c) management maintains an up-to-date list of the processes by which users are granted to each system;
 - d) management audits all users with access to CPSC systems and confirms group access settings are accurate;
 - e) management should not use shared administrator accounts; and
 - f) management should ensure that all Access Control policies and procedures are disseminated to all resources with significant access control roles and responsibilities.
- 5) Management should implement a tool that uniquely identifies and authenticates devices before establishing a connection to the CPSC GSS. This solution should facilitate IEEE 802.1X.

- 6) Management should authorize and document all devices that do not require authentication prior to connecting to the CPSC network.
- 7) Management should create separate non-administrative user accounts for administrators and require administrators to use these accounts when performing tasks that do not require administrative privileges.
- 8) Management should systematically require all users accessing the CPSC network to use multifactor authentication.
- 9) Management should implement the Principle of Least Privilege for the GSS LAN.
 - a) The agency should define and document the functions/duties that have a significant impact on agency operations and assets (*e.g.*, create users accounts, modify firewall rules, modify antivirus settings, reset passwords, modify DHCP, etc.)
 - b) The agency should revoke access to all users who have, but do not require, access to the functions defined above.
 - c) The agency should review the logs of all admin/super user accounts and restrict this access if these levels of privilege are not specifically necessary to perform required job functions.
 - d) The agency should document the system controls in place (*e.g.*, blocked ports, restricted protocols, etc.).
 - e) The agency should document the specific access controls in place for providing/controlling access required for the duties, functions, and system restrictions described above. Documentation can be access control policies (*e.g.*, identity-based policies, role-based policies, attribute-based policies, etc.).
 - f) Management should require administrators to use a non-administrative user account to perform tasks that do not necessitate the use an administrator account.
- 10) Management should implement a solution that allows the agency to report on the specific privileges assigned to each AD and E-Directory user account. These reports should be granular enough to report on which security function management assigns to each user account. Management should perform periodic audits of these reports to ensure access remains appropriate.
- 11) Management should limit administrators' access to update audit logs and implement a solution to monitor changes to the audit logs and notify the CSIRT team in the event of an audit log modification.
- 12) Management should implement a solution to monitor actively tasks performed by resources with approved conflicting duties.
- 13) Management should develop and implement workflows within cpsc.gov to coincide with the roles defined within cpsc.gov. The workflow should require the approval of all published Web content from a separate, independent, and appropriate CPSC resource.

14) Management should restrict access to the non-public data housed in CPSRMS to users with a business need for this access.

15) Management should implement a process to establish and control the use of shared user accounts.

a) Management should implement a formal process to approve the creation of new common user accounts.

b) Management should implement a formal process to disable common user accounts once no longer required.

c) Management should implement a formal process to establish membership in the common agency accounts.

d) Management should implement a formal process to change the common user account's credentials once a member separates from the agency or changes job functions and no longer requires access to the account.

e) Management should grant administrators local administrative accounts to each CPSC server individually, instead of using the system administrator accounts. Management should check-in/check-out the passwords to the global system administrator accounts only when this access is required.

f) Management should implement a formal process to require management to change the credentials on shared administrator accounts whenever a user with knowledge of these credentials separates from the CPSC or changes job functions.

g) Management should require periodic password changes on all common accounts.

16) Management should revoke all separated users' access to E-Directory, AD, ITDSRAM, CPSRMS, and DCM.

17) Management should implement a solution to disable users systematically from all agency information systems after 30 days of inactivity.

18) Management should implement a centralized contractor database to track the on- and off-boarding of contractors.

19) Management should draft and implement an SOP that clearly defines the roles and responsibilities of all resources responsible for processing contractor separations. The SOP should also include guidance on how these departments coordinate with each other to perform their respective tasks.

20) Management should train the CORs, EXRM, and EXIT resources responsible for processing contractor separations on their respective contractor separation responsibilities.

21) EXRM should provide the EXIT representatives and program officials responsible for processing contractor separations with a weekly report of contractor separations. Management should formally reconcile the current separations, as indicated on the weekly EXRM contractor separation report, to all the CPSC IT system Access Control Lists (ACLs) to ensure the timely revocation of all user accounts.

22) Management should periodically review all AD, E-Directory, and major application user accounts to ensure that access remains appropriate.

23) Program managers should perform periodic user access audits to ensure that user privileges for all CPSC systems are and remain appropriate. Thereafter, program managers should report these results to the ISSO for record and maintenance purposes.

MANAGEMENT RESPONSE

Management provided oral comments.

Management concurred with the findings, conclusions, and recommendations described in the report.