U.S. CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

REPORT

Issued: November 15, 2011
Minor Edits Made: January 23, 2012

Federal Information Security Management Act Report
Table of Contents

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

FEDERAL INFORMATION MANAGEMENT ACT REPORT

EXECUTIVE SUMMARY

Office of the Inspector General's Results

To meet the requirements of the Government Information Security Reform Act (GISRA), and its successor, the Federal Information Security Management Act (FISMA), the U.S. Consumer Product Safety Commission's (CPSC's) 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 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 it, in conjunction with the independent reviews required by FISMA and audits with information technology aspects (CFO Act Audit), served as the basis for the IG's Fiscal Year 2011 evaluation. This review was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the GAGAS standards issued by the GAO.

This year's FISMA evaluation found that although much progress has been made, and the Consumer Product Safety Risk Management System (CPSRMS) and International Trade Data System Risk Assessment Methodology (ITDSRAM) both received security accreditations, the agency's General Support System (GSS LAN) is no longer authorized to operate, and there remains much work to do. It was noted that the current Authorization to Operate (ATO) for the GSS LAN expired on June 17, 2011, and management was unwilling to accept formally the risk posed by the operation of the GSS LAN with its current security posture. Therefore, an interim ATO was granted as of June 27, 2011, to allow for the continuity of operations until a full ATO could be obtained. A full ATO for the GSS LAN is anticipated by December 31, 2011. Granting a full ATO at that time is contingent upon the successful mitigation or reduction of risk associated with the three known high risk security weaknesses. The three weaknesses preventing the agency from granting a full ATO to the GSS LAN are: (1) multifactor authentication was not systematically required to access the VPN; (2) an Information System Contingency Plan (ISCP) was not documented and tested; and (3) baseline security configurations for agency hardware and software have not been documented and implemented yet.

Management plans to remediate fully the multifactor authentication security weakness in two phases. The first phase was substantially complete as of September 30, 2011. All high-risk users (authorized teleworkers) are now required to log in systematically to their laptops using the

Personal Identity Verification (PIV) card. Once authorized teleworkers were required to authenticate to the network using the PIV card, the risk was reduced to moderate. The second phase of this remediation will require nonteleworkers to authenticate to the GSS LAN using the PIV card. This phase is scheduled to be completed by December 31, 2011. The other high-risk security weaknesses preventing the GSS LAN's ATO are the lack of a tested ISCP and the lack of implemented baseline security configurations, both of which are scheduled to be remediated by December 31, 2011.

The OIG noted 65 findings (15 of which are high-risk issues) in this year's review; please see below for additional details. The IT challenges facing the agency are particularly relevant at the present time, as the agency is dealing with the implementation of the Consumer Product Safety Improvement Act (CPSIA), in general, and more specifically, with the CPSIA's particular impacts on the agency's IT operations; in addition, the agency is involved in the implementation of the public facing database (CPSRMS).

As was the case last year, the general theme of the reviews indicated a lack of quality system reporting, as well as insufficient evidence documenting the control activities performed by those responsible for the processes reviewed. These deficiencies, at least in part, resulted from inadequate and dated policies and procedures. In addition, the existing policies and procedures were not enforced throughout the fiscal year, and the tools to facilitate the required system reporting were inadequate. However, although many of the policies have been updated, and several of the procedures have been made more effective, these policies were not disseminated to all of the resources with key procedural responsibilities. Also, many more improvements to these documents are still required, as noted below. Additionally, to improve system monitoring and reporting, several new tools (*e.g.*, Zenworks, Novell Sentinel, Tenable) were deployed. However, these tools have not been implemented fully. Although there is a commitment to remediate these issues, management has indicated that sufficient resources are not available to address them adequately.

Remediation strategies have been developed to address these 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, the lack of baseline security configurations is preventing the agency from granting a full ATO to the GSS LAN. The CPSC is taking steps to ensure that the issue is remediated, including: implementing tools to catalog hardware and software on the network; drafting baseline configurations for the known hardware and software; and implementing tools to assess and report on known variances to the configuration baselines. However, much additional work is required to implement this process fully and to ensure that proper configuration management can be enforced.

Another example of remediation activity undertaken by CPSC management to eliminate existing vulnerabilities and improve overall system security is the proposed implementation of a Continuous Monitoring Plan. The implementation of this plan will result in the remediation of several vulnerabilities, simply due to the improvements required in system reporting to facilitate the Continuous Monitoring strategy. The improvement in the reporting, as well as the resulting analysis made possible by the enhanced reporting, will allow issues in other processes (such as

Remote Access governance, Identity Management, Security Awareness Training and Security Incident Reporting) to be identified, quantified, and remediated much more efficiently and effectively than currently is possible. This, in addition to the harmonizing of processes required for reporting, will result in a significant improvement in overall system security. However, it is important to note that these remediation tasks were scheduled to be implemented after the FISMA review in FY 2010, and they still have not been implemented fully.

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, lay out a framework for annual IT security reviews and reporting and remediation planning. FISMA seeks to ensure proper management and security for information resources supporting federal operations and assets. The Act requires Inspectors General to perform an annual independent evaluation of their agencies' information systems' security programs and practices.

To establish a baseline to help it meet the requirements outlined above, the CPSC's Office of the Inspector General (OIG) performed an independent audit of the CPSC's automated information security control procedures and practices in FY 2011. The requirements of the audit included:

-evaluating and testing the internal controls defined in the 2011 FISMA metrics (provided by OMB), evaluating related weaknesses and identifying the degree of risk for the related weakness;

-testing the effectiveness of the information security controls defined in the 2011 FISMA metrics on all of 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 2011 FISMA metrics;

-recommending improvements, where necessary, in security record keeping, internal security controls, and system security; and

-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, CPSRMS, and ITDSRAM applications controls, as defined in the 2011 FISMA metrics. The OIG used the NIST and OMB guidance referred to in the 2011 FISMA metrics to assess the security controls. The objective of the review was to determine whether the CPSC's automated information system was safeguarded adequately.

In its report, Audit of Automated Information System Security, 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. In addition, it was reported in 2001 that the CPSC did not have a capital budget for IT security. Without appropriate capital budget planning, Grant Thornton was concerned that CPSC's management might not be able to implement and maintain resources properly to ensure system safeguards.

To ensure proper coverage and mitigation of the risks identified by the OMB, the CPSC is required to perform its own testing procedures to assess the design and implementation of the OMB-defined FISMA requirements. (Please see the Scope and Methodology for additional details). The CPSC OIG reviewed the 2011 GSS LAN, CPSRMS and ITDSRAM Risk Assessments, Security Assessment Plans (SAPs), and SSPs (System Security Plan), as well as the ITDSRAM SAR, which were developed in-house to update the OIG's understanding of the current processes and procedures employed by the CPSC.

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

Scope and Methodology: The evaluation was conducted from August to October 2011. This evaluation consisted of a review of the following defined agency processes within the boundaries of the GSS LAN, CPSRMS and ITDSRAM applications:

- 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 review constitutes both a follow-up of the findings and recommendations resulting from earlier audits, as well as a review of the CPSC's implementation of the IT security criteria as currently defined by FISMA. However, this year's review does not consider the status of the CPSC Data Privacy Program, as current OMB guidance no longer requires 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.

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 normally are addressed by management were not implemented fully. OMB Circular A-130, Appendix III requires sufficient management controls in these areas. This condition appears to have been due to CPSC management not having the necessary resources 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 systems and the inherent risk associated with operating these systems.

Actions Taken: Significant progress has been made since 2001 to address this issue, but gaps remain. The agency has assigned an Information Systems Security Officer and one staff member to oversee agency IT security. The agency has developed an Information System Security Plan (SSP) for each of the accredited systems (the GSS LAN, CPSRMS, and ITDSRAM). The agency hired outside consultants to perform independent security control assessments each year since the requirement was enacted by NIST 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 conforms to the NIST framework. This, in addition to the development of a System Development Lifecycle Plan (SDLC) and Business Continuity Plan adequately remediated all previous material weaknesses in those areas in FY 2003, and allowed the GSS LAN to obtain a full ATO in 2004.

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

In FY 2006, new security system requirements promulgated previously by NIST and OMB became mandatory. In order to retain accreditation and certification of its information systems, the CPSC was required to have its security controls independently tested and evaluated annually. Due to funding limitations this was not done in FY 2006.

In order to meet the accreditation and certifications requirements outlined above, and to determine whether the security controls identified for the CPSC Network General Support System in the System Security Plan were implemented correctly and effectively, during FY 2007, the Office of the Inspector General conducted a Security Test and Evaluation (STE Evaluation) in accordance with NIST SP 800-53. The STE Evaluation identified 63 vulnerabilities for the CPSC Network General Support System. Of these, six were found to be high-risk vulnerabilities; 31 were found to be medium-risk vulnerabilities; and 26 were found to be low risk vulnerabilities. The STE Evaluation Report included a planned mitigation with an associated due date for each vulnerability identified.

In FY 2008, the CPSC regained system certification. This was accomplished after the mitigation of the six high-risk vulnerabilities found in the STE Evaluation and the successful approval and testing of the CPSC's IT Contingency Plan.

In FY 2009, a fundamental problem with the CPSC's Plan of Actions 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 changes in 2009 had been made to help the agency address this shortcoming, historically, the POAM had not been used by the CPSC as an affirmative management tool in addressing security weaknesses. Although historically it had done a good job of documenting known security weaknesses and prioritizing them, the agency had not used the POAM to track or project the resources 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 it failed to take advantage of a powerful planning tool to address current and future IT security challenges. Moreover, as of the conclusion of the FY 2011 FISMA review, it was noted that the POAM still had not been implemented adequately. Milestones and milestone dates were not documented adequately for each of the known security weaknesses. Also, the related capital investments were not referenced adequately for each of the security weaknesses identified in the POAM.

Our FY 2009 review determined that the CPSC IT System had maintained its certification and accreditation and that the system's security controls, in the opinion of management, were tested and reviewed insofar as the agency monitored the system continuously. However, the Contingency Plan, again, had not been maintained and was not tested within 2009 or 2010. Due to changes to the agency operating environment since the drafting of this plan, management has decided that a new Business Continuity Plan is necessary. To address this issue, management has contracted an outside consultant, Evoke, to draft Information Contingency Plans (ISCP) for the GSS LAN and each of the accredited major applications. This project is scheduled to be completed by December 31, 2011. Once the ISCPs are drafted and tested, the agency is planning to develop a full Continuity of Operations Plan (COOP).

In FY 2010, the CPSC contracted SecureIT to perform the annual GSS LAN Risk Assessment, Security Test and Evaluation (ST&E), Security Assessment Report (SAR), and work on developing the SSP and defining a Continuous Monitoring process. This allowed the CPSC to identify risks, define compensating controls, and outline remediation actions. The agency extended this contract in 2011 and increased its scope to include the CPSRMS application; however, due to staffing constraints by the contractors, these assessments could not be performed by September 30, 2011. The independent security control assessments were scheduled to be (and were) completed on October 30, 2011. However, due to the timing of these assessments, the OIG was unable to include the results of these assessments in this report.

Also in FY 2010, it was noted that the Certification and Accreditation (C&A) policy did not define objective, measurable criteria that could be used to determine if an in-scope system could be certified and accredited, recertified and reaccredited, or conversely, decertified. Furthermore, although the C&A policy addressed a process to track continuously changes to information systems that may necessitate reassessment of control effectiveness, as defined by SP 800-37, no process currently in place to track continuously and document the results of these changes. Additionally, as of the FY 2011 review, the policy still has not been updated.

Risk Management Review:

It was noted that the C&A policy does not include the following key NIST required elements: the process by which entities coordinate to perform critical risk management tasks (*e.g.*, how entities determine the risk to business processes or the organization as a whole); the requirement for agency officials to review and update these policies periodically; the frequency with which policies and procedures must be reviewed/updated; and how often the policies and procedures are to be disseminated to resources with key policy responsibilities.

Furthermore, the C&A policies do not address the creation of the Risk Executive (function) role or the governing body, required to provide oversight of the risk management process. Without these functions in place and without their roles defined and established clearly, the organizational perspective of risk may be lost. Moreover, although the C&A policy requires the agency to create a Risk Management Strategy, and although the policy outlines what typically is included in a Risk Management Strategy (*e.g.*, the tools and procedures used to assess risk within the agency, the process by which risks are prioritized, the process by which risk is monitored and Organizational Risk Tolerance), this policy does not define what must be included in the agency's Risk Management Strategy or the procedures for developing such a strategy.

Moreover, the Enterprise Architecture (EA) process was not developed fully, nor was it integrated effectively into the agency's risk management process. Also, the process to define and accept risk when authorizing operation of a system is inadequate. No guidance has been included in any of the agency policies, procedures, or plans to ensure that existing risks are within the organizational risk tolerance. Without independent criteria, such as organizational risk tolerance, to provide guidance on what is considered an acceptable risk, the decision to authorize a system to operate is not justified sufficiently. Currently, there is an informal process to determine whether the risk associated with operating an information system is deemed acceptable. If the information system has no high-risk security weaknesses, the risk of operating the system is deemed acceptable. The decision to assign criticality to the security weaknesses on the POAM was based on an undocumented, informal risk assessment performed by the CPSC security team in conjunction with the control assessors.

It was also noted that the security documents were not maintained consistently and did not satisfy fully the OMB and NIST documentation requirements. Control descriptions in the CPSRMS and ITDSRAM SSPs did not provide sufficient detail. Additionally, it was noted that the GSS LAN, and CPSRMS Security Assessment Plan do not document how the selected assessment procedures are to be optimized in order to ensure maximum efficiency. Moreover, the GSS LAN security documents (the GSS LAN SSP, SAR, and Risk Assessment) were not maintained throughout the year to provide an up-to-date view of the GSS LAN security posture. The GSS LAN security documents were not updated for 9 1/2 months prior to the interim ATO being granted to the GSS LAN. Additionally, a major change was made to the GSS LAN environment on March 11, 2011, when CPSRMS was implemented. However, the GSS LAN security documentation was not updated accordingly, as is required. Periodic security status reports, which document the assessment of control effectiveness and changes to the GSS LAN/major applications, were not developed and presented to the Authorizing Officials, Risk Executive (function) and Information System owners, as required by NIST SP 800-37. The annual security control assessment and accompanying SAR, required by the C&A policy, were not performed and documented for the GSS LAN and CPSRMS application. Therefore, the GSS LAN and CPSRMS Risk Assessments were not updated to include the results of the security control assessment, in FY 2011. Moreover, continuous monitoring reports were not developed and distributed to senior management or OMB on a periodic basis, as prescribed by OMB M 10-15.

Risk Management Recommendations:

1. The agency should develop standalone Risk Management policies and procedures or update the C&A policy and ensure that it includes the following additional components:

(a). The requirement for a governance structure to be implemented 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 within the governance of the risk management process.

(b). What must be included in the agency's Risk Management Strategy (e.g., tools and procedures used by the agency to assess risk, the process by which risk is prioritized, how organizational risk tolerance is to be defined and measured against, and how risk is going to be monitored throughout the year).

(c). The process by which the Enterprise Architecture is used in the risk management process.

(d). The process by which decisions at the business process and solutions level are guided by the impact to the organization (*e.g*., the creation of an Executive Risk Council).

(e). A requirement that the authorization decision for an information system is based on the system's operation within the defined organizational risk tolerance.

(f). Identifying who is required to sign off on the ATO and to whom the security authorization documents are disseminated.

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

(h). A requirement for the periodic review and updating of information security policies and procedures should be documented in a separate governing policy or within the individual policies.

(i). The frequency with which the organization reviews/updates the policies and procedures should be documented in a separate governing policy or in the individual policies.

(j). The frequency with which the organization disseminates formal documented procedures to elements within the organization having associated roles and responsibilities.

(k). A distribution list and a requirement that the policies be distributed to all resources with key responsibilities outlined in the policies or procedures.

2. Develop and document a robust risk management process, which is lead by a Risk Executive (function) and reports to a governing board that includes senior management. The Risk Management Strategy should be developed and implemented using the NIST SP 800-37 guidance to ensure all key requirements are included.

3). The organization-wide Risk Management Strategy should be developed and include:

(a). techniques and methodologies that 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 that the organization plans to use to evaluate the significance of the risks identified during the risk assessment;

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

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

(e). how the organization plans 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 that the organization plans to use to ensure that the risk management strategy is being carried out effectively.

4). Additionally, an addendum should be added to each of the SARs, as the NIST SP 800-37 guidance suggests, providing agency officials with the opportunity to comment on the assertions made by the independent assessors. This will provide management with an opportunity to document the differences of opinion between the independent assessor and the CPSC Security Team. This will also allow agency management to justify any decisions not to include items deemed high-risk security vulnerabilities by the independent assessors in the POAM.

5). The functional descriptions of the security controls for CPSRMS and ITDSRAM applications must be updated to include sufficient detail to allow an assessor to test the control without obtaining further clarification from the developers. These control descriptions must include planned inputs, expected behaviors, and expected outputs. Additional guidance for this process is outlined in NIST SP 800-37. Moreover, control owners should be identified based on IT system responsibilities, and the control owners should be responsible for maintaining the control descriptions to ensure the information is as current as possible. Additionally, all changes to the security controls by the control owners should be approved by the Security Team.

6). The agency should develop a process for consolidating and combining selected assessment procedures for the GSS LAN and CPSRMS, where possible.

7). The agency should document the process for consolidating and combining selected assessment procedures in the GSS LAN and CPSRMS Security Assessment Plan.

8). The GSS LAN SSP should be updated each time a change with a security impact is made to the GSS LAN, such as the implementation of CPSRMS. The GSS LAN SSP should be updated regularly and serve as a "living document," representing the most up-to-date security information related to the GSS LAN. Additionally, the formal Risk Assessment, along with all other security documents, should be updated each time a major change occurs to the system; and these documents should be used in any decision to reaccredit the system or authorize the system to operate.

9). The agency should satisfy all high-risk security weaknesses and obtain a current Authorization to Operate for the GSS LAN.

10). Security status reports should be developed to describe the results of the ongoing monitoring activities performed by the agency. These reports should address vulnerabilities in the information systems and their environments of operation discovered during the security control assessment, Security Impact Analyses, and security control monitoring activities. Additionally the security status reports should include how the agency intends to address those vulnerabilities. At a minimum, the security status reports should describe or summarize key changes to SSPs, SARs, and POAMs, as well as the results of the scans described in the Continuous Monitoring Plan. This information may be combined with the continuous monitoring reports required by the OMB on a monthly basis to make the process more efficient.

11). The Authorizing Official, System Owners, and Risk Executive (function) should be presented the security status reports on a periodic basis to determine whether a formal reauthorization action is necessary.

12). The agency should perform the security control assessment on the selected NIST SP 800-53 controls for the GSS LAN and CPSRMS application, as soon as possible.

13). Perform the security control assessment on the selected NIST SP 800-53 controls for the GSS LAN and CPSRMS application as soon as possible, and update the Risk Assessments based on these results, and present this information to the Authorizing Official and System Owner.

14). As per OMB M 10-15, continuous monitoring reports should be developed and provided to the OMB on a monthly basis. Additionally, the Information System Owners and Chief Information Officer should be presented with these continuous monitoring reports for their review on a monthly basis, to assist them in managing actively the risks that are known.

The monthly Continuous Monitoring Reports should include the following information, as prescribed for in the Continuous Monitoring Plan:

(a). the results from monthly configuration management scans (FDCC scans, as well as, scans for compliance with all of the relevant information systems (*e.g.*, Microsoft Windows Server 2008, Research In Motion (RIM) Blackberry Server, Database Servers, Web Servers);

(b). the results from monthly vulnerability scans (Patch management compliance, client vulnerability and server vulnerability scans);

(c). the results from monthly asset management scans which identify hardware and software assets on the network; and

(d). the results from the event and incident management processes. This process includes the identification of unauthorized privileges, unauthorized access, stagnant accounts, and unauthorized hardware/software.

POAM Review:

In FY 2010, it was noted that the GSS LAN POAM was not formalized and implemented fully, and program officials were not notified of the progress of the security issues identified in the GSS LAN POAM. Although gaps still remain, the agency has implemented formally a POAM for the GSS LAN and has made the following improvements in this area: how the security weaknesses are identified is now documented and mapped to the source document; a scheduled completion date for each security weakness is now documented, although undocumented changes to this date are made; a remediation activity owner has been assigned to each security weakness; resources and timeline requirements are now documented; and agency officials are now provided with quarterly updates on changes to the GSS LAN POAM. Additionally, some remediation milestones are documented, although changes to milestones, and the related justifications, are not tracked and documented. Moreover, the estimated funding resources required to remediate the security weakness, as well as the source of that funding, are not documented consistently. In addition, GSS LAN POAM items, which are associated with investments identified in the IT Investment portfolio, do not include Unique Project Identifiers (UPIs) that allow agency officials to trace the security weakness to the budget documentation.

It was noted in the FY 2011 assessment that the CPSRMS and ITDSRAM applications used POAMs to document and track material security weaknesses. However, the ITDSRAM was missing the following OMB-04-25 required information: key milestones (along with their associated completion dates); the estimated funding resources required to resolve the weakness; the agency's justification for the costs associated with the remediation activity; and changes to milestones tasks/dates.

It was also noted as part of the FY 2011 assessment that the agency had not performed an annual security control assessment for the GSS LAN and CPSRMS by September, 30, 2011, as is required by NIST. Therefore, the agency could not document the security risks and vulnerabilities that may have been uncovered as a result of these assessments in the latest version of the POAM. The CPSC should perform and document a formal review of its technical security controls on a regular basis and include the results of these assessments in the agency POAMs.

POAM Recommendations:

1). 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). The "Estimated Completion Date" should be static—once created, it should not change. The actual completion date should be documented in the "Status" field in the POAM, if different than the estimate.

3). The key milestones documented in the POAM should include an estimated completion date for all of the security weaknesses tracked on the POAM.

4). All changes to the milestones or milestone dates should be documented in the POAM.

5). POAM items that are associated with investments identified in the IT Investment portfolio should include UPIs to allow agency officials to trace the security weakness to the budget documentation (*This recommendation also appears in the Security Capital Planning section of the report*).

6). All fields defined within the SharePoint tool used to track the security weaknesses should be completed for each security weakness.

7). The following information should be captured in the ITDSRAM POAM for all security weaknesses associated with the ITDSRAM application: key milestones (along with their associated completion dates); the estimated funding resources required to resolve the weakness;

the agency's justification for the costs associated with the remediation activity; and changes to milestones tasks/dates.

Continuous Monitoring Review:

Although a security control assessment was performed in FY 2010, and was documented in the SSP, a full Continuous Monitoring strategy had not been approved or implemented at that time. Additionally, documented policies and procedures for continuous monitoring did not exist. Therefore, an outside vendor, SecureIT, was engaged to develop a Continuous Monitoring Plan. The project to draft this document began on January 1, 2011, and was concluded on August 15, 2011, with the approval of the 2011 Continuous Monitoring Plan.

It was noted, however, that the Continuous Monitoring Plan was not implemented. Security Impact Analyses (SIAs) are not performed on system changes. Also, a tool set to facilitate the continuous monitoring reporting was requested and obtained by the CPSC Security Team; however, due to funding issues, procurement was delayed and the tools were not implemented fully by the end of FY 2011. As such, the agency does not inventory hardware and software adequately, report on configuration management compliance, and report on patch management compliance and system vulnerabilities.

The reports outlined in the Continuous Monitoring Plan cannot be developed and presented to the Authorizing Official for periodic review due to the lack of SIAs and properly documented configuration management, patch management, and system vulnerability scans. Additionally, the annual Security Control Assessments for the GSS LAN and CPSRMS application were not performed and the annual Security Status Report was not drafted and presented to the Authorizing official as required by the Continuous Monitoring Plan.

Continuous Monitoring Recommendations:

1) Develop and implement an OMB/NIST compliant Continuous Monitoring Policy and attendant procedures. These should include requirements to monitor logs actively, detect unauthorized elevation of privileges, identify unauthorized devices on the network, and monitor consistently the security architecture for vulnerabilities.

2). Security Impact Analyses (SIAs) should be performed and the results documented, for all system changes and reported in the Security Status Reports. (*This recommendation also appears in the Configuration Management section of the report*).

3). Deploy the Zenworks tool to all clients and develop and maintain a current inventory of all client hardware and software. (*This recommendation also appears in the Configuration Management section of the report*).

4). Implement fully the Tenable solution to facilitate the development of a current inventory of all non-client hardware and software. (*This recommendation also appears in the Configuration Management section of the report*).

5). The Tenable tool should also be implemented fully to assess and report on the results of the vulnerability scans; to assess compliance with the agency's configuration baselines; and to assess compliance with the agency's patch management program. (*This recommendation also appears in the Configuration Management section of the report*).

6). Continuous monitoring reports, based on the information gathered in recommendations 1–4, should be presented to the Authorizing Official and should include the results of the system scans, as well as critical events identified as part of the Incident Management process (e.g., identification of unauthorized privileges, unauthorized access, stagnant accounts, and unauthorized hardware/software).

7). A security control assessment should be performed for the GSS LAN and CPSRMS application. The results of this assessment should be documented in the GSS LAN and CPSRMS SARs, and these resulting changes should be documented in the Security Status Reports.

8). The annual Security Status Report should be drafted and presented to the Authorizing Official.

Contingency Planning Review:

In FY 2010, it was noted that the agency had not formalized or tested a Business Impact Analysis (BIA), Business Continuity Plan (BCP), Disaster Recovery (DR) Plan or Information System Contingency Plan (ISCP) for the GSS LAN. This was still not remediated as of the FY 2011 assessment. This is one reason the GSS LAN lost its security certification. However, in September 2011, the agency hired a contractor, Evoke, to develop an ISCP for the GSS LAN and CPSRMS. According to management, this remediation will reduce the risk sufficiently to allow agency officials to accept the residual risk and recertify the GSS LAN. These plans are scheduled to be completed and tested by December 30, 2011. In FY 2010, it was noted that data backups were not restored periodically to ensure that data had not become corrupted. This was remediated in FY 2011, and the agency now restores backup media on a quarterly basis.

It was also noted that no formal policies and procedures exist that govern the contingency planning process. These policies and procedures are expected to be finalized by December 30, 2011. Additionally, 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 Cyber Incident Response Plan, as required by NIST SP 800-34. Each of these, except the Cyber Incident Response Plan, will be completed as part of the Evoke contract; however, a completion date for these tasks was not formally established. The Cyber Incident Response Plan is expected to be developed in-house; however, an estimated completion date was not established.

The alternative storage site is approximately 11 miles away from the agency's primary data center. Due to this close proximity, the alternative storage site is subject to the same threats as the primary site. The agency has decided to accept the risk associated with the close proximity because the cost would be too high to locate these facilities in another geographic region. It was also noted that the agency has not established an alternative processing site. Evoke has been contracted to assist the agency in establishing an alternative processing site; however an estimated completion date was not formally established for this project.

Contingency Planning Recommendations:

1). Develop and implement an OMB-/NIST-compliant Continuous Monitoring Policy and attendant procedures. Input should be solicited from each CPSC department to ensure proper policy coverage.

2). Train all apposite resources on the continuity planning responsibilities assigned to them in the policy.

3). Perform, document, and approve a formal Business Impact Analysis, in accordance with NIST SP 800-34.

4). Develop, test, and approve an agency COOP, in accordance with NIST SP 800-34.

5). Develop, test, and approve an agency DR Plan, in accordance with NIST SP 800-34.

6). Develop, test, and approve an agency BCP, in accordance with NIST SP 800-34.

7). Develop, test, and approve an agency Cyber Incident Response plan, in accordance with NIST SP 800-34.

8). Develop and test an ISCP for the GSS LAN and its major applications, in accordance with the criteria set forth in NIST SP 800-34 and NIST SP 800-53, CP-2.

9). The required testing frequency of the COOP, BR, BCP, and ISCP plans should be documented in the SSP.

10). After-action plans should be drafted to document the lessons learned identified as part of the COOP, DR, BCP and ISCP plan testing.

11). The agency should select and establish an alternative storage site located in a different geographic region than the primary storage site.

12). Establish an alternative processing site with the equipment and supplies required to resume operations to support delivery to the site in time to support the organization-defined time period for resumption.

Contractor Systems Review:

In FY 2010, the agency did not have documented policies and procedures to govern the oversight of contractor systems. These policies still did not exist as of the completion of the FY 2011 review. The CPSC does not outsource its systems to parties outside the federal government and all intergovernmental IT relationships are governed through Memorandums of Understanding (MOUs), Interconnect Security Agreements (ISAs), and Statements of Work (SOWs). It was noted in FY 2010 that a third party inventory was not maintained formally by the agency. This was remediated during FY 2011, and a comprehensive list of third party systems that interconnect with agency systems has been formalized and is being maintained by the agency.

Contractor System Recommendations:

Policies and procedures should be developed, approved, implemented, and maintained by EXIT to ensure that appropriate oversight exists for IT systems operated by contractors or others on the agency's behalf. These policies/procedures should address expressly how security controls of third party IT systems are implemented and comply with federal and agency guidelines. The policies/procedures should include the following:

1). A requirement for all systems to be inventoried and third party systems identified.

2). A requirement that all third party systems have their interfaces identified and documented in the inventory.

3). Approval requirements for the third party inventory (e.g., the agency official responsible for reviewing and approving the inventory should be identified and documented. The frequency with which the inventory requires review and approval should also be documented).

4). The process by which the FISMA requirements are to be built into the third party contracts (please see Government Information Security Reform Act of 2000 for details on what must be included in government contracts).

5). The process by which system boundaries will be defined and documented.

6). What will be done to ensure that adequate security controls are in place for each of the third party IT systems (*e.g.*, agency roles responsibilities for the SSAE 16 user control testing for each of the in-scope third party IT systems).

7). Documentation requirements for the agency's ISAs with the contracted third parties (*e.g.*, what information the agency requires in the ISA).

8). Documentation requirements for the agency's MOUs with the contracted third parties (*e.g.*, what information the agency requires in the MOU).

9). Agency security requirements for the third party system (*e.g.*, what happens if the third party system loses its security accreditation?).

10). A process to ensure that the contractor remediates any security weaknesses identified on agency POAMs associated with third party IT system.

Security Capital Planning Review:

In FY 2011 it was noted the Security Capital Planning process is governed by the general Capital Planning and Investment Controls (CPIC) policies and procedures. It was noted that the CPIC policies and procedures generally meet the requirements set forth in the NIST SP 800-65 (Integrating IT Security into the Capital Planning and Investment Control Process) guidance. The policy documents, however, do not meet all of the NIST SP 800-53 and OMB M 11-33 requirements. Although these documents require that each development project include the costs associated with all aspects of the security program, including POAM costs, specifics for how these costs are to be cross-referenced to the budget materials sent to OMB in the fall are not codified, as is required by OMB M-11-33. Additionally, the policy and procedures do not require that the budget documents include a discrete line item for security costs, as is required by NIST SP 800-53, SA-2.

Moreover, 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, the agency was at Stage 1 of the ITIM framework and partially compliant with the stage two requirements. Although the agency was not reassessed this year, it was noted that the documented policies and procedures have not been implemented fully.

The agency uses contract services for the 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 the implementing system security. Earned Value metrics are designed and used to monitor project progress against the project milestones/plans for large projects, which is the method the agency uses to ensure security is properly implemented. For smaller projects and projects that are managed entirely in-house, an informal process is used to monitor progress against project milestones. It was also noted that Exhibit 300s (IT Capital Asset Plans) require the agency to indicate if Earned Value Management (EVM) is required for a particular contract or task order and for exceptions to be documented.

Additionally, it was noted that the Investment Review Board (IRB) is responsible for prioritizing all facets of agency 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 security is prioritized adequately, the Information System Security Officer (ISSO) is a voting member in the weekly IT management prioritization meetings, which are held, in part, to prepare investment recommendations for the IRB. Moreover, the ISSO participates in the IRB in a nonvoting capacity.

IT security has not been assigned a separate budget. Instead, security is funded on a project-by-project basis, and the project security costs are included in the project component line items within the Work Breakdown Structures (WBSs), which relate to the security requirements. To ensure funding is available to maintain the level of security identified in the investment documents, funding for security is allocated to each project component with an associated security component.

It was noted, however, that although IT Security is a central feature in the IT Infrastructure investment, a discrete line item for IT security does not appear in the budget documentation for the IT Infrastructure investment. Additionally, resources required to implement the configuration management security requirements associated with the IT Infrastructure investment are not explicitly documented in the capital planning and investment request or related budget documents. Furthermore, the security weaknesses, with associated projects documented in the CPSC POAMs, do not all tie to the Investment budget documentation. The POAMs do not include the associated UPIs, as required by OMB M-11-33; and a spend plan has not been developed for the IT Infrastructure investments that can be used to tie the security costs associated with the POAMs to the budget documentation.

Security Capital Planning Recommendations:

1). Policies/procedures should be developed/enhanced and implemented to ensure that POAM items related to projects in the IT Investment Portfolio are properly cross-referenced to the budget materials sent to OMB in the fall, including the Exhibits 53 and 300s. An example of how this may be accomplished is to require that a discrete line item be included for IT security in all WBSs, Spend Plans, and/or Exhibit 300s. Additionally, policies/procedures should be enhanced and implemented to require that the investment Unique Project Identifier (UPI) be documented in each POAM. This will allow a specific investment on the Exhibit 53 to be tied to all of its related POAM items.

2). The policies/procedures should be enhanced and implemented to require all POAMs that reflect estimated resource needs for correcting reported weaknesses 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.

3). The budget documentation for each investment should include a specific reference for all of its related POAMs.

4). A spend plan, which includes a discrete line item for IT security costs, should be developed for the IT Infrastructure and Commission Information System (CIS) investments as it has been developed for the CPSRMS investment. Additionally, the individual investment project plans should roll up to, and tie to, the spend plan.

2. Security Operational Controls

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

CPSC management not having the resources necessary to make implementation of operational controls a priority. The level of risk was rated "high" for personnel security and data integrity.

Prior Recommendation: CPSC Management should implement sufficient operational controls in the area of personnel security, data integrity, and documentation to ensure efficient and effective management of the IT systems in support of 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 contracted with Patriot to develop the Information System Security Plan (SSP) in 2002. Patriot reported that in order 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) would be needed. Qualifications and responsibilities for each position were delineated in the 2003 SSP. The CPSC has since hired an Information System Security Officer and provided him with one staff member to implement and maintain the SSP requirements. The remaining responsibilities are contracted out on an "as needed" basis. However, it was noted that additional internal resources are required to implement and maintain the SSP requirements adequately.

In FY 2007, OMB mandated that agencies adopt security configurations for Windows XP and VISTA, as well as a policy for ensuring that 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, this policy was not fully implemented; attendant procedures were not fully developed, and configuration baselines were not all implemented.

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

In FY 2009, it was noted that peer-to-peer training should be added to the training curriculum. The agency has remediated this in FY 2011, by providing the CPSC resources peer-to-peer training as a separate training module.

Configuration Management Review:

As a result of the OIG's follow-up on actions taken to remediate prior findings, as well as the testing for the FY 2011 FISMA review, several new findings were noted. Although the agency baselined Windows XP in FY 2011, and it also implemented the U.S. Government Configuration Baseline (USGCB) [formally, the Federal Desktop Core Configuration (FDCC)] recommended configurations for Windows XP, baseline configurations were not properly documented or implemented for other agency software or hardware components. This includes IE7, which is required explicitly by the USGCB. The agency expects to release Windows 7 on December 30, 2011. In order to achieve compliance with the USGCB requirements, the agency is working to implement the USGCB-required configurations for Windows 7 and IE8, prior to the Windows 7 release in December. Additionally, the inventory of configuration baselines is incomplete, and a process was not developed to ensure that all critical hardware and software are baselined.

Although significant progress was made and tools were partially implemented to facilitate the agency in its efforts to develop and maintain a software/hardware inventory, the software/hardware inventory process is not mature yet. The agency is in the process of implementing a tool set that will allow a comprehensive software/hardware inventory to be developed; however, these tools were not fully implemented, and a comprehensive software/hardware inventory was not developed. This has prevented the agency from ensuring its baseline configuration inventory is complete. Furthermore, local administrative access to clients was not adequately controlled throughout the year, which increases the risk that unknown and unsecured software has been installed on the agency's network. Also, without a comprehensive software inventory and adequate restrictions on local administrative access to clients, the agency is not able to achieve adequate property accountability. This is because software license compliance is impossible to ensure without these tools and controls in place.

As mentioned earlier, SIAs are not adequately performed and documented for each system change. The change control forms, which require completion prior to the change being implemented, do not provide enough information to make an accurate determination of how security will be affected as a result of the change. The resources who are performing and documenting the changes are not security experts. Because they are not experts, they are not qualified to complete the "How Security Affected" section in the change control form. Additionally, not all changes are approved by the ISSO prior to implementation. Therefore, an assessment cannot be adequately performed to determine the security impact to the operating environment and control framework.

It was also noted that the agency has formalized a patch management and change management policy. However, the agency does not audit the activities associated with system change control. Also, currently audits are not performed to identify all missing patches. The tools used for assessing compliance with the patch management process were not fully implemented at this time. However, once the scanning tools are fully implemented, monthly audits will be performed, and the results will be documented as part of the Continuous Monitoring process. This process is expected to be fully implemented as of December 30, 2011.

It was also noted that development environments are not in place for workstations and servers, where changes and patches can be adequately tested prior to deployment. When a patch or change is implemented on a workstation, it is tested on roughly five "test" workstations that are not connected to the network. However, this is insufficient for adequately testing the change. Additionally, a development environment has not been implemented to test server patches and changes.

Configuration Management Recommendations:

1). Procedures should be developed and formalized to standardize the implementation of the Configuration Management process. The Configuration Management procedures should include the following:

(a). timeframes in which the agency must remediate/accept identified baseline variances;

(b). the process by which the agency software requiring configuration management is identified and inventoried;

(c). the process by which the agency hardware requiring configuration management is identified and inventoried. The procedures should include how EXIT interacts with the business owners to identify the hardware requiring configuration management.

(d). the process by which the agency identifies all systems and system components that will not be baselined. Currently, the policy refers to all "information systems"; however, not all information systems will be baselined; instead, the agency will determine the systems that require baselines and develop the configuration baselines accordingly.

(e). what information must be included in each configuration baseline SOP (*e.g.*, configuration settings, patch level, Software Load and Version, system architecture, where the resource resides on the network).

2). The CPSC should develop an inventory of software and hardware requiring baselining, and the process for developing this inventory should be documented in a procedure document. This should be done with the assistance of the business owners. Mission-essential functions and systems should be identified by the business owners, and this information should be provided to EXIT. EXIT should then identify and inventory the software and hardware associated with these functions.

3). The CPSC should establish and document mandatory configuration settings for information technology products employed within the information system, using defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

4). Implement the configuration settings.

5). Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system, based on explicit operational requirements.

6). Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

7). The agency should implement the Zenworks and Tenable tools on all agency clients and servers to develop and maintain a current and comprehensive software/hardware inventory. The software/hardware inventory then should be used to develop an inventory of all required software/hardware baseline configurations.

8). The Tenable and Zenworks tools should also be used to facilitate the other OMB-directed monthly reporting requirements. These reporting requirements include the results of configuration management compliance, patch management compliance, and vulnerability scans.

9). The agency should identify and remove all unauthorized software from the network.

10). Periodic audits should be performed on the software inventory to ensure that baseline configuration documents are up-to-date.

11). The process for managing IT software requests should be improved. One of the methods of doing this would be with the implementation of an automated tool (*i.e.*, SharePoint), which houses all of the IT software request information and software licensing information. This tool should also be used to obtain and document software request approvals and systematically require approval by the appropriate resources prior to closing/completing the new software request.

12). The process for granting local administrative access to users should be improved and administrative rights should be limited to only those who require the local admin access to perform core functions of their job. The process can also be improved by performing periodic audits to ensure only appropriate users have been assigned local admin access.

13). Develop and enforce a process to govern software license compliance:

(a). Document a comprehensive software inventory.

(b). Document the number of instances in which each type of software is installed on the network.

(c). Document and inventory all software licenses owned by the agency.

(d). Reconcile the software instances installed on the network with the software licenses owned by the CPSC, and remediate any discrepancies.

(e). Perform periodic audits to ensure future compliance.

14). All USGCB/FDCC variances, along with a plan for remediation, should be documented, and any known residual risk accepted.

15). Require sufficient granularity in the change requests to allow the security resource responsible for the walkthrough and approval of the change to justify the approval decision.

16). For all system changes, perform and document a formal Security Impact Analysis (SIA), which includes sufficient granularity to allow the security resource responsible for the approval of the change to justify the approval decision. The SIA should capture all relevant system security changes and be included in the change management packet, and the ISSO should approve all changes.

17). All unremediated security vulnerabilities identified as part of the SIA should be documented in the POAM.

18). Production changes should be audited to ensure that changes have been adequately tested, documented, and approved.

19). Audits should be performed to identify all missing patches and the results of these audits should be included in the Continuous Monitoring reports to OMB. The missing patches should then be implemented. If the agency decides not to implement the missing patch, a formal justification should be provided.

20). Construct a development environment for workstations and servers, and test all patches and changes in these environments before deployment.

Incident Response and Reporting:

The agency developed and formalized an Incident Response Policy on August 20, 2011, although it was not implemented or disseminated to the resources with key responsibilities. Additionally, an Incident Reporting database was developed to track incident reports, and it resides on the IT Security SharePoint site. Incident Response procedures were documented in the Incident Reporting database; however, these procedures were not implemented and were not disseminated to the appropriate resources. The Computer Security Incident Response Team (CSIRT), Incident Response Team (IRT), Incident Coordination Handling and Management Team (ICHM), and Branch Analyst Team (BAT) defined in the Incident Response procedures were not established or trained on incident reporting responsibilities. The tasks assigned to each of these teams in the policies and procedures are not currently being performed. Without these teams established and team members trained to perform the functions outlined in the Incident Response procedures, assurance cannot be given that a comprehensive analysis, validation, and documentation of all security incidents has been performed.

It was noted that the CPSC security team has been tracking the security incidents when notified. However, the documented security incidents all do not include the following NIST SP 800-61-required elements: actions taken by the incident handlers, comments from incident handlers, a list of evidence gathered during the incident investigation, and the next steps to be taken. Also, remediation plans were not documented for each reported incident. Agency management asserts that, due to resource limitations, documenting a remediation plan for each incident is not practical.

Timeliness of the security team's response to Security Events cannot be attested to because not enough detail was included in the incident documentation. The incident documentation does not include the time and date the security team was notified; therefore, the OIG could not assess how long it took from security team notification to response. This process will eventually become the responsibility of an IRT once the procedures are fully implemented.

Several security incidents were identified that were open for more than a month prior to resolution and closing. Additionally, one incident has been open for more than a month and is still open. This circumstance has been attributed to the agency's failure to implement the incident response policies and procedures. The lack of adequate resources dedicated to the incident response process has restricted the agency's ability to resolve these issues in a timely manner and minimize further damage that might result.

It was also noted that the agency has not developed and implemented a Forensic Incident Response Policy, and the current Incident Response Policy does not include law enforcement notification requirements. Additionally, on several occasions, the United States Computer Response Readiness Team (US-CERT) was not notified in accordance with the timeframes outlined in the Incident Response Policy and in the federal guidelines for the documented incidents.

Additionally, nothing is in place to monitor for internal actions that may constitute threats, such as attempts to obtain unauthorized administrator rights. Moreover, although VPN and firewall logs are maintained and alerts are sent in the event of certain predefined security incidents, these logs are not actively monitored and analyzed. Currently, logs have to be pulled from each server, which is a labor-intensive process, making it impractical to perform and report on such analysis regularly. The implementation of Novell Sentinel is expected to remediate this issue. Sentinel was deployed as of June 1, 2011; however, it has not been fully implemented. Agency management is in the process of refining its Incident Response Policy. Once this has been done, Sentinel will be configured to monitor the parameters set forth in the policy. This is expected to be completed by December 30, 2011.

Incident Response and Reporting Recommendations:

1). The agency should develop and implement a Forensic Incident Response Policy and attendant procedures. These policies should include requirements for reporting an incident to law enforcement, in addition to all the other NIST SP 800-86 requirements. Additionally, how quickly law enforcement must be notified, based on a predetermined event, should be explicitly documented in the policy. For example "In the event of a lost or stolen laptop, US-CERT and law enforcement must to be notified within one hour."

2). The Incident Response policy and procedures should be fully implemented and disseminated to all users with key incident response and reporting responsibilities.

3). The CSIRT, IRT, IHCM, and BAT teams should be established, and team members should be trained on the tasks assigned to each of them.

4). Implement the TIC (Trusted Internet Connection) initiative. This will improve security and incident response, by reducing and consolidating external network connections and allowing the central monitoring of network traffic for malicious activity, across the government. Agencies are required to use one of four service options under TIC: A single service model, a multiservice model, a hybrid approach, or seek services from another provider.

5). Implement the Einstein 2 product. This will monitor for specific predefined signatures of known malicious activity at federal agency Internet connections and alert US-CERT directly when specific malicious network activity matching the predetermined signatures is detected, allowing the CPSC to use US-CERT expertise.

6). Implement the Novell Sentinel product. This will improve the reporting capabilities of the firewall and VPN logs and allow for a meaningful analysis of both internal and external network activity.

7). Ensure that each report of a security incident includes all of the NIST SP 800-61-required information.

8). US-CERT and law enforcement should be notified within the prescribed timeframes. Additionally, all security incidents should be reported to the ISSO immediately upon discovery and be tracked in SharePoint going forward. This includes VPN and Firewall alerts (based on a TSNE defined set of criteria). Incidents should be filtered through the HEAT Ticketing system to the ISSO SharePoint so that all incidents are tracked and remediation documented. Additionally, the TSCS team should log all incidents with security ramifications through HEAT and into the SharePoint solution.

9). A remediation plan should be documented for all reported security incidents.

10). All actions taken to address security issues should not only be date-stamped, but they also should be time-stamped.

11). Document the time and date the security team/IRT was first notified of the incident in the SharePoint tool used to monitor the incidents.

Security Training:

Security Awareness and Training policies and procedures are missing one key element; however, these documents are much improved over last year's review. The training policies and procedures were updated and approved on August 10, 2011; however, they do not include the requirement that the agency 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 two training courses, one for personnel within the IT department with significant information security responsibilities, and one for all other CPSC personnel. Additionally, the training provided to the non-IT personnel was not designed to address IT security from a System Development Lifecycle (SDLC) perspective, as required by NIST SP 800-16.

Additionally, it was noted that the agency used a different solution to provide security awareness training in FY 2011 than it did in FY 2010. The solution used in FY 2011 is capable of accurately reporting on the security training completion statistics that remediated the reporting issues that arose last year.

It was also noted that only 67.5 percent of CPSC personnel completed their security awareness training in FY 2011. This is substantially less than the 90 percent completion rate that OMB requires. This has been a recurring problem. As the consequences defined in the policy are not enforced, the CPSC resources have not prioritized the completion of this training.

Security Training Recommendations:

1). The agency should develop a NIST SP 800-16-compliant training program.

(a). The Security Awareness and Training and procedures should require each "user group" defined within the agency to be provided security training specifically developed for their role within the agency.

(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). Revoke access to all users who have not completed the security awareness training until the training is complete, as is provided for in the Security Awareness Training policy.

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, the CPSC management left sensitive information vulnerable. This condition appears to have been due to CPSC management not having the resources necessary to make implementation of sufficient technical controls a priority. The level of risk was rated high for identification and authentication and logical access.

Prior Recommendation: CPSC management should implement sufficient technical controls in the areas of identification and authentication, logical access, and audit trail in order to protect the information that is used to support the 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. Management was advised of specific weaknesses and recommendations, each of which was to be addressed during the implementation of the SSP and Systems Certification and Accreditation contract. Weaknesses outlined in the SSP were to be corrected in all applications. Additional systems were not tested because management was in the process of implementing prior recommendations, the implementation of which would alter the policies and procedures applicable to all applications. As reported in the management response to the original audit, the CPSC requested, without success, funding in fiscal years 1999 through 2002, to establish a capital budget for information technology. The need for such funds was also included, unsuccessfully, in the CPSC's FY 2003 and 2004 budget requests. Budget requests cited the need for new investments to protect the current operating capability and efficiency of information technology. According to the Budget Officer, in the absence of a capital budget for information technology, the CPSC has applied some savings from operating funds to this area. In FY 2002, the CPSC committed more than $500,000 from one-time salary savings to this area 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 EXIT commitment was $714,891 in the form of 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 2010, the CPSC's commitment rose again to $18,884,618 [$9,371,016 for EXIT-IT (which included the creation of a 'sub-budget' for Capital Replacement of $1,000,000) and $9,513,602 for EXIT-Administration Services (EXIT-AS) respectively] and 34 FTEs. In FY 2011, the agency was reorganized, and Administration Services is no longer a part of EXIT. Therefore, the aggregate spend on EXIT decreased; however, due to the IT modernization effort, the CPSC's commitment to the EXIT IT common costs rose again to $13,787,040. FTEs also increased from 34 in FY 2010 to 36.6 in FY 2011. Work on implementing the recommendations contained in the SSP and more recent guidance continues.

The CPSC acknowledges its need for continued improvement. Over the past few years, the CPSC has met the following goals in its effort to improve its security technical controls: implementing a security awareness training program; providing a redundant cooling capability to the agency's existing computer room air conditioning unit; providing the ability to recover quickly from an e-mail server failure by periodically taking and storing e-mail "snapshots" of the e-mail database; implementing the ability to perform automated system auditing; implementing the monitoring of Internet usage; implementing multifactor authentication for users with remote access to the VPN; implementing a solution to restrict access to client USB ports by nonencrypted flash drives; and implementing a tool that allows the agency to inventory all network user accounts.

Remote Access Management review:

Formal documented policies for authorizing, monitoring, and controlling remote access were developed and formalized in FY 2011. However, it was noted that Remote Access Management policies had the following weaknesses. A list of the security functions and security-related information that can be accessed remotely must be included. It also must document the additional controls in place to ensure that these functions are not misused. Additionally, the Remote Access policies must list the organization-defined networking protocols that are deemed to be nonsecure and must require the agency to route all remote traffic through managed access points. It is important to note that the agency is aware of the requirement to route all remote traffic through managed access points, and it has decided to formally accept the associated risk.

Additionally, although Teleworking and Remote Access procedures have been developed, they 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. Also, it was noted that the procedures do not document a process to ensure that each remote access infrastructure component (*i.e*., servers, gateways, authentication servers) has its clock synched to a common time source, so that its time stamps will match those generated by other systems. Additionally, 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 policy and procedures. Anomalies should be reported to other systems' administrators, as appropriate. Furthermore, procedures in place for monitoring remote access are inadequate. VPN and firewall logs are not reviewed to monitor remote access, although alerts are sent to engineers in the instance of select predefined security events. CPSC management has attributed this to current system limitations, making the active monitoring of these logs impractical; management has also attributed this to an overall lack of resources.

Additionally, the policy and procedures are not fully implemented. The Remote Access Policy states that remote sessions time-out after 30 minutes of inactivity; however, sessions are configured to time-out after 90 minutes of inactivity. The agency is aware of this and has decided to accept the risk associated with the 90-minute-session lock-out. The agency has a policy that requires all sensitive information to be encrypted prior to being sent outside of the internal network; however, the agency has not implemented a tool to facilitate compliance with this requirement. Therefore, there is an extremely high likelihood that users send unencrypted, sensitive files over public networks.

It was also noted that not all users are uniquely identified and authenticated to the network. A formal process was not implemented to control the establishment of common E-Directory and

AD accounts. Additionally, credentials are not changed on these accounts when users separate from the agency or change job functions. Moreover, generic administrator IDs are being used by the Network Engineering Team and the Computer Support Team. Furthermore, the tasks performed by the administrator while using these IDs are not being monitored. Agency resources who have administrative rights, access the GSS remotely, using administrator accounts. No separate accounts have been created for these users to telework or perform nonadministrative tasks.

Additionally, reports of lost or stolen devices with access to the CPSC network are not adequately documented or tracked. For example, a Blackberry telephone was lost on July 1, 2011; however, the ISSO, who is responsible for notifying US-CERT, was not notified of this incident until August 9, 2011, more than 1 month after its occurrence. Per OMB M-7-16, US-CERT is required to be notified within 1 hour of detection.

FY 11 Remote Access Management Recommendations:

1). The following elements should be added to the Remote Access policy:

(a). the list of security functions and security-related information that can be accessed remotely;

(b). the controls employed by the agency to ensure that these functions and data are not misused; and

(c). the specific audit procedures the agency uses to ensure that the controls are effective.

2). The agency should draft a list of network protocols that it deems to be insecure and restrict the access to these protocols. Additionally, these protocols should be documented in the Remote Access policy/procedures.

3). The following criteria should be added to the Remote Access procedures and implemented:

(a). checking for upgrades and patches to the remote access software components, and acquiring, testing, and deploying the updates;

(b). ensuring that each remote access infrastructure component (*e.g*., servers, gateways, authentication servers) has its clock synched to a common time source so that its time stamps will match those generated by other systems.

(c). reconfiguring access control features, as needed, based upon factors such as policy changes, technology changes, audit findings, and new security needs;

(d). detecting and documenting anomalies identified within the remote access infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators, as appropriate.

4). The agency should follow the documented Remote Access Policy and the NIST-mandated 30-minute lock-out requirement for remote sessions.

5). The agency should comply with NIST requirements and route all remote traffic through managed access points.

6). All nonrequired common E-Directory and AD user accounts should be disabled.

7). All agency-accepted common user accounts should be documented and approved.

8). A formal process should be implemented to approve the creation of new common user accounts.

9). A formal process should be implemented to establish membership in the common agency accounts.

10). A formal process should be implemented to disable common user accounts once they are no longer required.

11). A formal process should be implemented 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.

12). The common user account inventory should be reviewed periodically to ensure common user accounts remain appropriate and that membership to these user accounts remains appropriate.

13). Administrators should be granted local admin accounts on each of the machines. Only one person should know the System Administrator password, and the password should be checked in/checked out when this access is required.

14). A formal process should be implemented that requires the credentials on shared administrator accounts to be changed whenever a user with knowledge of these credentials separates from the CPSC or changes job functions.

15). Actively monitor remote user access. This may be facilitated by the implementation of the Novell Sentinel (or equivalent) tool. Additionally, results of these analyses should be reported to the ISSO.

16). Create separate nonadministrative user accounts for administrators, and require the administrators to use these accounts when they are performing tasks that do not require administrative privileges.

17). Implement a tool (*e.g.*, Acceleron) to allow agency resources to encrypt sensitive documents prior to transmission across a public network, and train users of the tool.

18). Perform periodic audits to ensure compliance with the policy of encrypting sensitive documents prior to transmission across a public network.

19). All security incidents should be reported to the ISSO immediately upon discovery and tracked in SharePoint. This includes VPN and Firewall alerts (based on a TSNE defined set of criteria). Incidents should be filtered through the HEAT Ticketing system to the ISSO SharePoint so that all incidents are tracked and remediation is documented. Additionally, the TSCS team should log all incidents with security ramifications through HEAT and into the SharePoint solution. (*This recommendation also appears in the Incident Response and Reporting section*).

Identity and Access Management review:

The agency formalized the General Access Control policy on August 10, 2011. However, it was noted that General Access Control policy did not include roles and responsibilities and how the agency coordinates access control responsibilities among the CPSC branches. Additionally, it was noted that the procedures outlined in the policy document did not include the following key elements: the process by which network accounts are established and controlled; the process by which common/shared network accounts are established and controlled; the process by which temporary, emergency, and guest accounts are established and controlled; the process by which the agency establishes and controls system accounts; and account modification procedures. Furthermore, it was noted that individual system access control SOPs for the agency's major applications are not referenced in the General Access Policy. Even more, an Access Control Policy and attendant procedures were not developed for CPSRMS.

It was also noted that although the General Access Control Policy was formalized, it was not fully implemented. The General Access Control Policy requires that agency management audit all users with access to the CPSC systems and confirm that group access settings are accurate and that the results are submitted to the ISSO for record and maintenance purposes. However, this is not being done.

The CPSC GSS does not uniquely identify and authenticate network devices before establishing a connection to the CPSC GSS. The agency is in the process of implementing a solution, which is expected to remediate this issue. The solution is scheduled for implementation on December 30, 2011.

The CPSC users are not all required to access the network using multifactor authentication. However, the agency has restricted remote access to the network without the use of multifactor authentication and is planning on limiting local access without multifactor authentication by December 30, 2011.

Because a formal process has not yet been defined, users are being established without proper authorization from EXRM. Additionally, access modifications are not always made based on formal management requests.

The agency has not implemented the Principle of Least Privilege for CPSRMS. All CPS360 users can view all incident reports, even those which were not approved for Public consumption, whether or not their job function required access to these data views. 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, the Principle of Least Privilege cannot be applied. There are only two types of network accounts: typical user accounts (with no access to any security function) and administrator accounts (with access to all security functions). If a user has administrator access, they can perform all security functions even if their specific job function does not require this ability. Additionally, administrators have sufficient access to perform system administration and access and alter the audit logs.

It was also noted that the process for disabling network accounts immediately upon an employee or contractor's separation from the agency is not being implemented consistently. Employees and contractors who have previously separated from the agency have been identified by the OIG as still having access to the network. The weakness in the process of disabling contractor accounts immediately upon contractor separation has been attributed to the lack of due diligence on the COTRs who are responsible for notifying EXRM of the contractor's departure. Additionally, a centralized contractor database, housing HR information such as hire and departure dates, which EXRM can readily query, currently, is not employed. The lack of a centralized database to track contractor departures limits EXRM's ability to effectively notify clearing officials of all separating contractors on a periodic basis, which would mitigate much of the risk of this manual process.

As is also noted in the Remote Access Management section, a formal process was not implemented to control the establishment of common E-Directory and AD accounts. Additionally, credentials are not changed on these accounts when users separate from the agency or change job functions. Moreover, generic administrator IDs are used by the Network Engineering Team and Computer Support Teams.

Also mentioned previously, it was noted that the agency uses common network accounts. However, the purpose of several of these common network accounts was not known to management at the time of the review, and some accounts were enabled that had not been logged into since 2001. As a result of this review, the agency has disabled and removed several of the common network accounts deemed to be inappropriate. However, a process should be instituted that requires all common user accounts to be inventoried and reviewed periodically for continued legitimacy.

Identity and Access Management Recommendations:

1). Update the policy to include roles and responsibilities and to document how access control tasks are coordinated among CPSC branches. Also, this document, along with the related SOPs should be disseminated to all users with key access control responsibilities.

2). The following elements should be included in the General Access Control Policy and procedure documents:

(a). The process by which common network accounts are established and controlled. This should include how common/anonymous accounts are authorized and monitored.

(b). The process by which temporary, emergency and guest accounts are established and controlled. This should include guidance on how guest/temporary are authorized and monitored. The process for notifying account managers when temporary accounts are no longer required should also be defined, in addition to deactivating temporary accounts that are no longer required.

(c). The process by which the agency establishes and controls system accounts.

(d). Specific procedures for the establishment and modification of user accounts, including a requirement for all new administrators to follow the formal user access request process.

(e). Individual system access control SOPs should be referenced in the General Access policy.

2). Draft, approve, and implement NIST compliant Access Control policies and procedures for CPSRMS.

3). ITTS Branch Chiefs and program managers should perform periodic user access audits to ensure that user privileges remain appropriate. These results should be reported to the ISSO for record and maintenance purposes.

4). Implement a tool (*e.g.*, StillSecure) that uniquely identifies and authenticates devices prior to establishing a connection to the CPSC GSS.

5). Require all agency users to use multifactor authentication to access the GSS LAN.

6). The agency should apply the Principle of Least Privilege to the CPSRMS application. The agency should enhance the role-based approach taken when CPSRMS was developed. The role matrix, which defines what privileges each role has been assigned, should be enhanced further to include what data-viewing rights users with these associated roles are allowed.

7). Implement the Principle of Least Privilege within the GSS LAN.

(a). The agency should define and document the functions/duties which have a significant impact on agency operations and assets (*e.g.,* create users accounts, modify firewall rules, modify antivirus settings, reset passwords, and modify DHCP)

(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).

(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 in the form of access control policies (*e.g.*, identity-based policies, role-based policies, attribute-based policies).

(f). Require administrators to use a nonadministrative user account to perform tasks that do not necessitate the use an administrator account.

8). Implement a solution that will allow 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 has been assigned to each user account. Periodic audits of these reports should be conducted to ensure access remains appropriate.

9). Limit administrator's access to update audit logs and implement and configure Novell Sentinel to audit changes to the audit logs.

10). Implement the Novell Sentinel tool and actively monitor tasks performed by resources with approved conflicting duties.

11). Revoke the separated user's access to E-Directory and AD.

12). Implement a solution to systematically disable users after 30 days of inactivity.

13). Develop, formalize, and implement an SOP that outlines exactly what the EXRM, COTR, and TSCS's responsibilities are related to revoking access for a departing employee and contractor.

14). Formalize a periodic review all E-Directory and AD user accounts (including common and system accounts) to ensure that only appropriate accounts are enabled.

15). TSCS should formally reconcile the current separations, as indicated on the weekly EXRM Staffing report, to all the CPSC IT system ACLs to ensure all user accounts are adequately revoked.

16). A central contractor database that maintains records of all current and separated contractors should be developed and linked to the FPPS application to allow adequate reporting of contractor separations.

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

After the STE Evaluation in FY 2007 resulted in the decertification of the CPSC's system, much work was put into regaining system certification, which was achieved in FY 2008. NIST 800-53 controls were incorporated by the agency, and future certification and accreditation work should have been consistent with the most recent NIST Special Publication requirements. It was assumed at this time that the remaining security vulnerabilities would be addressed as expeditiously as possible. However, in FY 2009, it was found that only five of the existing 63 vulnerabilities shown in the 2007 STE Evaluation were addressed. Moreover, the results of the ST&E performed in FY 2010 reflected a high number of control deficiencies [147 (≈56%) of the applicable 261 NIST 800-53 controls], which have to be addressed as soon as possible. In FY 2011, it was noted that the agency had not performed an independent security control assessment for the GSS LAN and its applications during FY 2011. Therefore, the status of all of these remediation efforts is not known at this time. However, it was noted that the security control weaknesses identified as a result of the FY 2010 review have not all been adequately remediated.

Performance Measure Recommendations:

An independent security control evaluation should be performed and the security weaknesses identified should be remediated to allow the agency to become compliant with the NIST SP 800-53 control requirements for the GSS LAN and its applications.

Security Capital Planning Management Response:

We appreciate the opportunity to review and respond to the Office of Inspector General's audit findings regarding Security Capital Planning. Thank you for your recommendations to improve our efforts to build security into every IT investment appropriately from the start. We concur with all of your recommendations and will build these recommendations into improvements in the management of our IT program. Following, is our response to each of the recommendations and points of improvement.

OIG Recommendation # 1: Policies/procedures should be developed/enhanced and implemented to ensure that POAM items related to projects in the IT Investment Portfolio are properly cross-referenced with the budget materials sent to OMB in the fall, including the Exhibits 53 and 300s. An example of how this may be accomplished would be to require that a discrete line item be included for IT security in all WBSs, Spend Plans, and/or Exhibit 300s. Additionally, policies/procedures should be enhanced and implemented to require that the investment Unique Project Identifier (UPI) be documented in each POAM. This will allow a specific investment on the Exhibit 53 to be tied to all of its related POAM items.

Response: We will modify our Capital Planning and Investment Control (CPIC) policy, processes, standards, and guidance to identify the linkage between the IT Investment (Exhibit 53 line item), IT project, and security POA&M item.

OIG Recommendation # 2: The policies/procedures should be enhanced and implemented to require all POA&Ms, which reflect estimated resource needs for correcting reported weaknesses, to specify whether funds will come from a reallocation of base resources or a request for new funding. While the POA&Ms will not be used as agency funding requests by OMB, a brief rationale should be provided when a request for new funding is contemplated.

Response: We are currently reviewing and anticipate establishing new processes to create and maintain POA&M items. We will include in these requirements dollar costs and/or staff hours to implement the item. In addition, we will identify the source of funding (*e.g.*, IT investment) to address the item and whether the item requires additional funding (*e.g.*, midyear or budget year request).

OIG Recommendation # 3: The budget documentation for each investment should include a specific reference for all of its related POAMs.

Response: IT governance improvements have generally focused in areas where the rate of change is the greatest and these investments (*i.e.*, CPSRMS, ITDS/RAM, cpsc.gov redesign) have spend plans. We will create spend plans for all of our major IT investments, including IT Infrastructure and CIS. The spend plans will include costed security work and reference POA&Ms, where applicable.

OIG Recommendation # 4: A spend plan that includes a discrete line item for IT security costs should be developed for the IT Infrastructure and Commission Information System (CIS) investments just as it has been developed for the CPSRMS investment. Additionally, the individual investment project plans should roll up to, and be tied to, the spend plan.

Response: IT governance improvements have generally focused in areas where the rate of change is the greatest and these investments (*i.e.*, CPSRMS, ITDS/RAM, cpsc.gov redesign) have spend plans. We will create spend plans for all of our major IT investments, including IT Infrastructure and CIS. The spend plans will include costed security work and reference POA&Ms, where applicable.