U.S. CONSUMER PRODUCT SAFETY COMMISSION

OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

REPORT

Issued: November 15, 2012

UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Memorandum

Date: November 15, 2012

TO : Inez Moore Tenenbaum, Chairman
Nancy A. Nord, Commissioner
Robert S. Adler, Commissioner

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Federal Information Security Management Act (FISMA) Evaluation

This year's FISMA evaluation found that management has made substantial progress in implementing the FISMA requirements. CPSC's General Support System (GSS LAN) regained its security accreditation on October 1, 2012, and the Consumer Product Safety Risk Management System (CPSRMS) has completed the security accreditation process, and retained its security accreditation. A substantial majority of CPSC users are now systematically required to use multi-factor authentication to access the VPN. Management drafted an Information System Contingency Plan (ISCP) for the GSS LAN and management has documented and implemented baseline security configurations for many of the key agency software components.

Although much has been accomplished, much remains to be done. The OIG noted that management has not had an independent security assessment performed for the International Trade Data System Risk Assessment Methodology (ITDSRAM) application, nor updated and approved its security documentation, nor accepted the risk of operating the application in FY 12. Management also has not fully implemented the NIST SP 800-37 Risk Management Framework. Management has not performed an assessment to identify all major agency applications; it is particularly important that management assess the Office of Epidemiology applications because of the potential of these applications containing Personally Identifiable Information. The OIG also noted 65 findings (12 high risk) in this year's review; please see attached report for additional details.

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

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

Christopher W. Dentel
Inspector General

Federal Information Security Management Act Report
Table of Contents

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

FEDERAL INFORMATION MANAGEMENT ACT REPORT

EXECUTIVE SUMMARY

Office of the Inspector General's Results

To meet the requirements of the Government Information Security Reform Act (GISRA), and its successor, the Federal Information Security Management Act (FISMA), the Consumer Product Safety Commission's (CPSC) Office of the Inspector General (OIG) contracted with Grant Thornton, LLP to perform an independent audit of the CPSC's automated information security control procedures and practices in Fiscal Year (FY) 2001. The audit included tests of entity-wide controls and six of the CPSC's 49 application systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology (NIST) 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, etc.), served as the basis for the OIG's Fiscal Year 2012 evaluation. The OIG conducted this review in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards (GAGAS) standards issued by the GAO.

This year's FISMA evaluation found that, although much work remains, management has made substantial progress in implementing the FISMA requirements. CPSC's General Support System (GSS LAN) regained its security accreditation on October 1, 2012, and the Consumer Product Safety Risk Management System (CPSRMS) has completed the security accreditation process, and retained its security accreditation. Management successfully mitigated or substantially reduced the risks associated with the three high-risk security weaknesses that prevented the GSS LAN from obtaining an Authorization to Operate (ATO) in FY 11. Multi-factor authentication to access the Virtual Private Network (VPN) is now systematically required for a substantial majority of the CPSC users, management drafted an Information System Contingency Plan (ISCP) for the GSS LAN, and management has documented and implemented baseline security configurations for many of the key agency software components.

Although much has been accomplished, much remains to be done. The OIG noted that management has not had an independent security assessment performed for the International Trade Data System Risk Assessment Methodology (ITDSRAM) application, nor updated and approved its security documentation, nor accepted the risk with operating the application in FY 12. Management also has not fully implemented the NIST SP 800-37 Risk Management Framework. Management has not accredited the following major CPSC applications: PRISM,

FOIAExpress, and Integrated Field System (IFS). Management has not performed an assessment to identify all major agency applications; it is particularly important that management assess the applications associated with the Office of Epidemiology because of the potential of these applications containing Personally Identifiable Information. The OIG also noted 65 findings (12 high risk) 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 deals with both the implementation of the Consumer Product Safety Improvement Act (CPSIA) in general, and with the CPSIA's specific impacts on the agency's IT operations.

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

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

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

Another example of a remediation activity undertaken by CPSC management to eliminate existing vulnerabilities and improve overall system security is the continued improvement of the Continuous Monitoring Process. Although management has not fully implemented the Continuous Monitoring Plan, the security team is now providing monthly reports to senior management outlining the known risks to agency IT resources. This process will continue to improve as management optimizes its current tool set and improves system reporting. An effective Continuous Monitoring Process, once implemented, will result in the remediation of several other vulnerabilities, simply due to the improvements required in system reporting to facilitate the Continuous Monitoring strategy. The improvement in system reporting, in addition

to the resulting analysis made possible by the enhanced reporting, will allow management to identify, quantify, and remediate weaknesses in other processes (such as Remote Access governance, Identity Management, and Security Incident Reporting) much more efficiently and effectively than is currently possible. This, in addition to the harmonizing of processes required for reporting, will result in a significant improvement in the overall system security.

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 Office of Managament and Budget (OMB) policy, lays out a framework for annual IT security reviews, reporting and remediation planning. FISMA seeks to ensure proper management and security for information resources supporting Federal operations and assets. The Act requires Inspectors General to perform an annual independent evaluation of their agencies' information systems security programs and practices.

To establish a baseline to help it meet the requirements outlined above, the CPSC's Office of the Inspector General (OIG) performed an independent review of the CPSC's automated information security control procedures and practices in FY 12. The requirements of the review included:

-Evaluating and testing the internal controls defined in the 2012 FISMA metrics (provided by OMB).

-Testing the effectiveness of the information security controls defined in the 2012 FISMA metrics on all the CPSC’s accredited, or previously accredited systems.

-Assessing whether the CPSC's information security policies, procedures, and practices comply with the Federal laws, regulations, and policies outlined in the 2012 FISMA metrics.

-Recommending improvements, where necessary, in security record keeping, internal security controls, and system security.

-Identifying the degree of risk associated with identified internal security controls weaknesses.

The review included tests of the entity-wide, system specific, and hybrid controls for the GSS LAN, CPSRMS, and ITDSRAM applications, as defined in the 2012 FISMA metrics. The OIG used the NIST and OMB guidance referred to in the 2012 FISMA metrics to assess the design and effectiveness of the CPSC security controls. The objective of the review was to determine whether the CPSC's automated information system was adequately safeguarded.

In its report, the OIG identified security weaknesses in the CPSC's management, operational, and technical controls policies, procedures, and practices. The conditions of these controls could permit the modification or destruction of data, disclosure of sensitive information, or denial of services to users who require the information to support the mission of the CPSC. In addition, as previously reported in 2010 and 2011, the CPSC again did not have a capital budget for IT

security in 2012. Without appropriate capital budget planning, management may not have the ability to properly implement and maintain resources 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. The CPSC OIG reviewed the 2012 GSS LAN and CPSRMS Security Assessment Plans (SAPs), and System Security Plan (SSPs), Security Assessment Reports (SARs), as well as the ITDSRAM SSP. Management did not contract an independent review of security controls in 2012 nor did they develop a SAR or associated Risk Assessment for the ITDSRAM solution. Therefore, the OIG could not review these documents.

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

Scope and Methodology: The OIG conducted this evaluation from August to October of 2012. 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 evaluation constitutes both a follow-up of the findings and recommendations resulting from earlier audits, and a review of the CPSC's implementation of the IT security criteria as currently defined by FISMA. However, this year's evaluation does not consider the status of the CPSC Data Privacy Program, as current OMB guidance again this year does not require this reporting by the OIG.

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

The OIG conducted this evaluation in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the GAGAS standards issued by the GAO.

RESULTS OF EVALUATION

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

1. Security Management Controls

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

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

Actions Taken: Management has made significant progress since 2001 to address this issue, although gaps remain. Management hired an Information System Security Officer to oversee IT security. Management developed a SDLC plan and a Business Continuity Plan in FY 03. Management also developed an Information System Security Plan (SSP) for the CPSC's General Support System (GSS LAN) in FY 03. This adequately remediated all previous material weaknesses and allowed the GSS LAN to obtain a full ATO in FY 04. Management is currently in the process of hiring another Information Systems Security Officer to assist with the oversight of IT security. The agency has also developed an SSP for each of the accredited major applications (CPSRMS and ITDSRAM) in addition to the GSS LAN. The agency contracted outside consultancies to perform independent security control assessments each year for the GSS LAN since NIST enacted the requirement in 2006, except for Fiscal Years 2006, 2009, and 2011. The agency has also developed and formalized, although not fully implemented, a policy and procedure for establishing a certification and accreditation process, which generally conforms to NIST Framework.

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

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

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

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

In FY 09, a fundamental problem with the CPSC's Plan of Action and Milestones (POAM) was found. OMB has determined that agency POAMs must reflect known security weaknesses within an agency and, ". . . shall be used by the agency, major components, and program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps." Although management had made changes in 2009 to help the agency address this shortcoming, the agency has not historically used a POAM as an affirmative management tool in addressing security weaknesses. Although it had historically done a good job of documenting known security weaknesses and prioritizing them, the agency had not used a POAM to either track or project the resources required or milestones necessary to address these weaknesses (as required by the OMB). As a result, the agency lacked historical data regarding its past efforts and failed to take advantage of a powerful planning tool in addressing current and future IT security challenges. Moreover, as of the conclusion of the FY 12 FISMA review, management still had not adequately implemented the POAM. Management did not document milestones and milestone dates for each of the known security weaknesses. Also, management did not reference the related capital investments for each of the security weaknesses identified in the POAM.

Our FY 09 review determined that the GSS LAN had maintained its certification and accreditation and that the system’s security controls were, in the opinion of management, tested and reviewed in-so far as the agency continuously monitored the system. However, management had not updated or adequately tested the Contingency Plan in 2009, 2010, or 2011. Due to changes to the agency operating environment since the drafting of this plan, management decided that a new Information System Continuity Plan was necessary. To address this issue,

management contracted an outside consultancy, Evoke, in FY 11 to draft Information System Contingency Plans (ISCP) for the GSS LAN and selected applications. Although management did not perform a functional test, as NIST requires, management performed a tabletop test of the GSS LAN ISCP, and documented the after-actions plans of the ISCP in November 2011. Now that management has drafted the GSS LAN ISCP, the agency is planning to complete a Business Impact Analysis, establish an alternative processing site, and develop a Continuity of Operations Plan (COOP).

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

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

Risk Management Review:

Management has not fully developed and implemented Risk Management Policies and procedures. The agency's current policies and procedures do not include key elements related to the risk management process, and management has not reviewed/updated these policies and procedures in FY 2012. The policies do not include how entities coordinate amongst themselves to perform critical risk management tasks (e.g., how entities determine the risk to business processes or the organization as a whole). The risk management policies do not require that agency officials review and update these policies periodically, nor do they define how often the policies and procedures must be reviewed/updated. Moreover, management has not codified the frequency with which management has to disseminate the policies and procedures to resources with key responsibilities.

Furthermore, the C&A policies do not address the creation of the Risk Executive (function) role or another governing body required to provide oversight to the risk management process. Without these functions in place, and their roles clearly defined and established, the organizational perspective of risk may be lost. Moreover, although the C&A policy requires the agency to create a Risk Management Strategy, and the policy outlines what is typically included

in a Risk Management Strategy (the tools and procedures used to assess risk within the agency, how management prioritizes risks, how management monitors risk, and Organizational Risk Tolerance, etc.), this policy does not define what management must include in the agency's Risk Management Strategy, or the procedures for developing that strategy.

Management has not developed an Enterprise Architecture (EA) or integrated EA into the agency's risk management process. Management has also not developed an organizational risk management strategy. The process in place to define and accept risk when authorizing a system to operate is inadequate. Management has not included guidance in any of the agency policies and procedures to ensure existing risks are within the organizational risk tolerance. Without independent criteria, such as the organizational risk tolerance, to provide guidance on what the organization consider an acceptable risk, management cannot adequately justify the decision to authorize a system to operate.

Management does not update security documents (the SSPs, SARs and Risk Assessments) throughout the year to provide an up-to-date view of the information systems' security posture and to provide a method of continuously monitoring those postures. Instead, management only updates these documents annually. In addition, management does not fully satisfy the OMB and NIST risk management documentation requirements. Management did not develop periodic security status reports to document the assessment of control effectiveness and changes to the ITDSRAM application, and present these reports to the Authorizing Official, Risk Executive (function) and Information System owner as required by NIST SP 800-37. In addition, management did not have an independent annual security control assessment performed, and an accompanying SAR developed, as required by the C&A policy for the ITDSRAM application in FY 12. Management also did not update the ITDSRAM SSP and Risk Assessment to include the results of the security control assessment, in FY 12.

Risk Management Recommendations:

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

a) The requirement for management to implement a governance structure to manage risk from an organizational, mission and solution level. [e.g., the Risk Executive (function) and related governance bodies (Executive Risk Council)]. This policy should also include the roles and responsibilities for each resource involved within the governance of the risk management process.

b) What management must include in the agency's Risk Management Strategy (e.g., tools and procedures used by the Agency to assess risk, the process by which management prioritizes risk, how management defines organizational risk tolerance and measures against that organizational risk tolerance, and how management plans to monitor risk throughout the year).

c) The process by which management integrates the Enterprise Architecture into 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. This process should include the creation of an Executive Risk Council and the integration of EA into the risk management process.

e) A requirement that management bases the authorization decision for an information system on the defined organizational risk tolerance.

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

g) A requirement for the periodic review and updating of information security policies and procedures.

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

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

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

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

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

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

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

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

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

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

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

4) Management should update the CPSC SSPs, SARs, Risk Assessments, and POAMs each time the agency makes a change with a security impact to a system. Management should regularly update the SSPs, and the SSPs should act as "living documents" that represents the most up-to-date security information related to the CPSC systems.

5) Management should have an independent assessment of the ITDSRAM security controls performed and management should document the results of this assessment in a SAR.

6) Management should update the ITDSRAM SSP to reflect the current security posture of the ITDSRAM application.

7) Management should develop a "Security Authorization Package" for the ITDSRAM application as outlined in NIST SP 800-37 and provide it to the System Owner, the AO, and the ISSO to certify.

8) Management should document the certification of the "Security Authorization Package" in an accreditation memo or in an annual Security Status Report.

POAM Review:

In FY 10, management had not formalized or implemented the GSS LAN POAM, and management had not periodically notified program officials of the progress of the security issues identified in the GSS LAN POAM. Although gaps remain, the agency has formally implemented a POAM for the GSS LAN and has made improvements in this area. In FY 11, Management began documenting the identified security weaknesses, and mapping those weaknesses to the source documents in a POAM. Management began documenting a scheduled completion date for each security weakness, assigning a remediation activity owner to each security weakness, documenting resources and timeline requirements for security weaknesses, and documenting some remediation milestones. Management also began providing agency officials with quarterly updates on the changes to the GSS LAN POAM. However, management does not consistently assign milestones and milestone dates to each security weakness or track changes to related milestones and milestone dates. Management does not document the estimated resources or the source of the funding required to remediate the security weaknesses and timeline requirements consistently. Management also has not integrated the funding of the POAM into the Capital Planning process.

In FY 11, the CPSRMS and ITDSRAM applications both utilized POAMs to document and track material security weaknesses. However, management had not included all of the OMB M04-25 required information in these POAMs. Management does not document milestone completion dates or changes to milestones and milestone completion dates in the CPSRMS POAM. Management also has not integrated the funding of the POAM into the Capital Planning process. In addition, management does not consistently include the following required information for each CPSRMS security weakness: the estimated funding resources required to remediate the weakness, the remediation funding source, and key milestones. Also, the contractors and program officials responsible for implementing the CPSRMS solution did not provide an updated POAM for CPSRMS to the Chief Information Officer (CIO) on a quarterly basis throughout FY 12, nor did they provide updates on the status of the CPSRMS POAM activities to the CIO on a quarterly basis. The ITDSRAM POAM also does not contain all of the required OMB M04-25 required information. The ITDSRAM POAM does not document key milestones and the estimated completion dates for each of these milestones or the source of the security weakness (e.g., internal program reviews, IG audits, GAO reports etc). The contractors and program officials responsible for implementing the ITDSRAM solution did not consistently provide an updated POAM for ITDSRAM to the CIO on a quarterly basis throughout FY 12, nor did they consistently provide updates on the status of the ITDSRAM POAM activities on a quarterly basis. In addition, the CIO does not centrally track and maintain the status of ITDSRAM POAM activities.

Management does not adhere to the estimated completion dates for each of the weaknesses identified in the agency POAMs. Although management did not document estimated completion dates for POAM milestones, they did consistently document an estimated completion date for the resolution of the security weakness related to the GSS LAN. However, the estimated completion dates documented in the GGS LAN POAM for 32 (64%) of the 50 open GSS LAN security weaknesses had passed. Additionally, in 22 (69%) of those 32 outstanding instances at least the estimated completion date is at least eight months overdue. Management also consistently documented the estimated completion dates for the security weaknesses documented in the CPSRMS POAM. However, the estimated completion dates documented in the CPSRMS POAM for all 10 open CPSRMS security weaknesses have passed. The ITDSRAM POAM does not consistently document the estimated completion dates for the known security weaknesses.

In FY 11, the agency had not performed an annual security control assessment for the GSS LAN and CPSRMS, as is required by NIST. Therefore, the agency did not document the security risks and vulnerabilities that management may have uncovered because of these assessments in the POAM. However, management had an independent assessment performed of the security controls for the GSS LAN and CPSRMS in FY 12 and documented the security weaknesses identified as a result of these assessments in the associated POAMs. Management did not have an independent assessment of security controls performed for the ITDSRAM application in FY 12. Therefore, the ITDSRAM POAM did not include the results of an independent review.

POAM Recommendations:

1) Management should update the C&A policy to include a requirement to review and approve the policy on an annual basis, or develop an entity level policy which requires all IT security policies and procedures to be reviewed and approved on an annual basis.

2) Management should perform a review of the C&A policy to ensure it is current.

3) Management should perform an assessment of the level of effort required for the remediation of each security weakness, and the results of that assessment should be reflected in the milestone/milestone dates and "Estimated Completion Date" fields in the associated POAMs.

4) Management should document the key milestones for all security weaknesses tracked on agency POAMs.

5) Management should document the dates associated with the key milestones for all security weaknesses tracked on the POAM.

6) Management should document all changes to the milestones or milestone dates in the POAM.

7) Security weaknesses documented in the POAM that are associated to investments identified in the IT Investment portfolio should include UIIs to allow agency officials to trace the security weakness to the budget documentation.

8) Management should complete all POAM fields for all security weakness.

9) Management should capture estimated completion dates, milestones, milestone dates, and changes to milestone dates along with the source of the identification of the security weakness in the ITDSRAM POAM.

10) Management should update the CPSRMS POAM, and maintain this information on the IT Security SharePoint.

11) Management should provide updates to the CIO on ITDSRAM and CPSRMS POAM activities on a quarterly basis.

Continuous Monitoring Review:

Although management had an independent security control assessment of the GSS LAN performed in FY 10 and documented the results in the SSP and SAR, management had not approved or implemented a Continuous Monitoring strategy. Additionally, documented policies and procedures for continuous monitoring did not exist. Therefore, in FY 11, management approved a Continuous Monitoring Plan developed by an outside vendor for the CPSC. Management also had an outside vendor develop the Continuous Monitoring Plan for FY 12. However, management did not approve the plan until October 2, 2012.

Management has made substantial strides in implementing the Continuous Monitoring program outlined in the plan. For example, management presents monthly reports to the appropriate program officials outlining current threats and the results of many of the existing continuous monitoring activities. However, management has not fully implemented the Continuous Monitoring Plan. The plan references a Risk Executive (function) that does not exist. Management only updates its SSPs and SARs once per annum, and these documents do not act as "living documents" that management can use to represent the system's current security posture at any given moment. Management does not perform Security Impact Analyses (SIAs) on all proposed and actual system changes and update the security documentation with the results of these assessments. The outside vendor did not perform quarterly configuration compliance audits throughout FY 12 and present the results of these audits to management for approval. Nor did the outside vendor develop and test a contingency plan for the CPSC as the Continuous Monitoring Plan requires.

In addition, management cannot develop all of the reports outlined in the Continuous Monitoring Plan and present them to appropriate program officials for periodic review. Although the CPSC Security Team has partially implemented a tool set to facilitate the continuous monitoring reporting, management has not yet optimized this tool set. As such, the agency does not adequately report its hardware and software inventory, fully report on configuration management compliance, or fully report on patch management compliance and system vulnerabilities. Moreover, management does not implement alerts and review logs to identify unauthorized access and privilege changes as required by the plan.

Moreover, management did not have an independent assessment performed on a subset of security controls for the ITDSRAM application in FY 12. Therefore, management could not update the ITDSRAM SSP, SAR, and Risk Assessment, and notify the appropriate program officials of the results of this assessment.

Continuous Monitoring Recommendations:

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

2) Develop and implement an OMB/NIST compliant Continuous Monitoring Policy and attendant procedures.

3) Management should perform Security Impact Analyses (SIAs) on all actual or proposed system changes. Management should documents these results along with the results from all other continuous monitoring activities in the monthly Security Status Reports. Management should also update the risk documentation accordingly.

4) Management should develop and maintain a comprehensive Enterprise Architecture (EA) and management should tie the approval of all system changes to their impact on the EA.

5) Management should deploy a solution to report on the agency's current inventory of hardware and software.

6) The periodic security status reports should include the results of the server configuration management scans, patch management scans, and a summary of the current hardware and software inventory.

7) Management should ensure that quarterly configuration compliance audits are performed and the results of these audits are presented to the ISSO. The results of these audits should be included in the Monthly Security Status Reports.

8) 8) Management should develop and test a Contingency Plan in accordance with the requirements outlined in NIST SP 800-34 as required by the CPSC's Continuous Monitoring Plan.

9) Management should review logs and implement alerts to identify unauthorized access and privilege changes. The results of these reviews should be included in the Monthly Security Status Reports.

10) Management should have an independent assessment performed on the ITDSRAM application. Management should record the results of this assessment in a Security Assessment Report and present this report to the CIO for review.

11) Management should draft an annual Security Status Report for the ITDSRAM application and present this report to the Authorizing Official and System Owner for certification.

Contingency Planning Review:

In FY 10 and FY 11, the agency had not formalized or tested a Business Impact Analysis (BIA), Business Continuity Plan (BCP), Disaster Recovery (DR) Plan or Information System Contingency Plans (ISCP). The lack of a tested ISCP in addition to the other reasons outlined in the Executive Summary, resulted in the GSS LAN losing its security certification in FY 11. Therefore, management documented an ISCP for the GSS LAN and CPSRMS application and performed a tabletop test on this ISCP in FY 12. Management later added the continuity procedures in the ISCP for ITDSRAM. According to management, the remediation task performed has reduced the risk sufficiently to allow agency officials to accept the residual risk and recertify the GSS LAN. However, management has not yet retested the ISCP. In addition, management did not perform a functional test of the ISCP as required by NIST SP 800-34. Moreover, management does not employ backup strategies to meet the Recovery Point Objectives (RPOs) documented in the ISCP.

In FY 10 and FY 11, no formal policies and procedures existed governing the contingency planning process. However, management finalized a Contingency Planning Policy in March of 2012 and updated it in September of 2012. Our review of the Contingency Planning Policy found that it did not enumerate the test, training and exercise (TT&E) program requirements required of it by FCD1, and that management had not fully implemented the Contingency Planning Policy. 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 established an alternative processing site as is required by NIST SP 800-34 and NIST SP 800-53. Management expects to complete each of these tasks on or before September 2013.

Contingency Planning Recommendations:

1) Management should enhance its Contingency Planning Policy and procedures to address all NIST and OMB requirements. EXIT management should solicit input from each of the CPSC departments when developing these policies and procedures to ensure proper coverage.

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

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

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

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

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

7) Management should perform a functional test the CPSC ISCP in accordance with FEMA and NIST guidance.

8) Management should implement a solution to allow management to meet the RPOs for all critical agency systems.

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

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

Contractor Systems Review:

Management formalized a policy to govern the oversight of contractor systems on August 7, 2012. Management also developed a comprehensive inventory of third party systems that interconnect with agency systems in FY 11 and management updated this inventory in FY 12. The CPSC utilizes Memorandums of Understanding (MOUs), Interconnect Security Agreements (ISAs) and Statements of Work (SOWs) to govern all inter-governmental IT relationships. However, in FY 12, the CPSC began to utilize a cloud-based Software as a Service (SaaS) solution provided by a non-governmental contractor, and the agency's Contractor Security Oversight policies and procedures do not outline the process by which management controls such cloud-based SaaS implementations. Also, management did not perform procedures to obtain assurance that the agency has implemented the user controls outlined in the GSA's Security Authorization Package for the cloud-based solution.

The CPSC interconnects with Department of Transportation (DOT) and Department of the Interior (DOI) systems. However, the CPSC, DOT, and DOI did not perform an annual update to these MOU/ISAs in FY 12 to ensure that the information contained within these documents is up-to-date. They should each review these agreements on an annual basis to ensure that the connecting systems continue to provide adequate security to allow the interconnection. In addition, management has never established an information system connection or processing agreement with a contractor who has client machines connected to the agency network. Management also did not verify the implementation of the security controls specified in the CPSC information security policies and security plan for this contractor.

Management has not fully implemented the Contractor Security Oversight Policy. Management has not established processes and procedures to track the various interagency service agreements and metrics applied throughout the lifecycle of the IT security services within the organization. Management does not notify the contracted third parties of intrusions, attacks, or internal misuse, so the third party can take steps to determine whether its system has been compromised. Management does not analyze audit logs (by an automated tool or manual review) to detect and track unusual or suspicious activity across the interconnection that might indicate intrusions or internal misuse. Management does not utilize automated tools to scan for

anomalies, unusual patterns, or known attack signatures and to alert administrators that the tools detected a threat. The ISSO or delegate does not periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize. EXIT does not coordinate contingency planning, training, testing, and exercises with any third party contractors to minimize the impact of disasters. In addition, management has not established joint procedures with the third parties based on existing contingency plans.

Contractor System Recommendations:

1) Management should update the Contractor Oversight Policies and Procedures to include the process by which management controls cloud-based SaaS implementations.

2) Management should establish processes and procedures to track various interagency service agreements and metrics that it applies throughout the lifecycle of the contracted IT security services within the organization.

3) Management should notify third parties of intrusions, attacks, or internal misuse, so the third party can take steps to determine whether its system has been compromised.

4) Management should include a requirement in each ISA compelling the connecting third parties to provide the CPSC with the known security weaknesses that might have an impact on the CPSC's mission.

5) Management should analyze audit logs to detect and track unusual or suspicious activity across the interconnections that might indicate intrusions or internal misuse.

6) Management should implement automated tools to scan for anomalies, unusual patterns, and known attack signatures and management should configure these tools to alert administrators if a threat is detected.

7) The ISSO or delegate should periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize.

8) Management should coordinate contingency planning, training, testing, and exercises with any third party contractors to minimize the impact of disasters.

9) Management should establish joint procedures with the interconnecting third parties based on existing contingency plans.

10) Management should perform and document an assessment to ensure that agency resources have adequately implemented the user controls outlined in the GSA's Security Authorization Package for the cloud-based SaaS solution the CPSC utilizes.

11) System owners and management should review and update the CPSC/DOI and CPSC/DOT MOU/ISAs on an annual basis. Once the System Owners provide the ISA/MOU to management, management should review the agreement for appropriateness and certify it if it meets CPSC

security standards. If the third parties with whom we are dealing fail to take the initiative in this area, CPSC management should initiate contact to ensure these agreements are current and active.

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

13) Management should verify the implementation of required security controls on the identified contractor system as specified in the organization's information security policy and security plan; or established an approved information system connection or processing agreements with the organizational entity hosting the external information system.

Security Capital Planning Review:

In FY 11, management documented a process to govern the CPSC's Capital Planning, and Investment (CPIC) process that generally meets the requirements set forth in NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*. However, as of the OIG review in FY 12, this process remains a work in progress, and management has not fully implemented this process. In addition, the policy and procedure documents do not meet all NIST SP 800-53 and OMB M 11-33 requirements. The procedures do not define how management integrates security into the CPIC process, or how management plans and budgets for on-going security costs, such as costs to perform the remediation activities outlined in the agency's POAMs.

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

The agency uses contract services for a vast majority of its IT projects. The contractors, who are responsible for developing the systems, in conjunction with the CPSC Security Team, are also responsible for implementing system security. Management has not recorded these costs as distinct line items, and management cannot trace these costs back to the Capital Planning and Investment documentation.

Additionally, the CPSC Investment Review Board (IRB) is responsible for prioritizing all facets of agency IT investments, including IT Security investments, against the agency mission. The consequent prioritization results in the decision to fund or withhold funding from a particular project for the next fiscal period. Furthermore, to ensure that management adequately prioritizes security in IT investments, the Information System Security Officer (ISSO) is a voting

member of the weekly IT management prioritization meetings that management holds, in part, to prepare investment recommendations for the IRB. Moreover, the ISSO participates in the IRB in a non-voting capacity.

Management has not assigned IT security a separate budget. Instead, management has funded security on a project-by-project basis, and not separated the project security costs into discrete line items. Although management allocates funding for security to each project according to the project components, management cannot trace these costs to the Capital Planning documents sent to OMB in the fall.

Security Capital Planning Recommendations:

1) Management should enhance and implement existing policies/procedures to ensure that the costs associated with remediating security weaknesses are properly cross-referenced to the capital planning materials sent to OMB in the fall. Management might accomplish this by creating a separate IT security project and assigning all IT security costs, including the costs associated with remediating existing security weaknesses, to this project. Once management has assigned the IT security costs to the IT security project, the details from the project should be included in the Exhibits sent to OMB in the fall. Additionally, management should enhance and implement existing policies/procedures to require agency personnel to document the appropriate investment's Unique Investment Identifier (UII) in each POAM. This will facilitate traceability from the agency's POAMs to its capital planning documentation.

2) Management should enhance and implement existing policies/procedures to require all POAMs to reflect the estimated resource needs for correcting reported weaknesses and to specify whether funds will come from a reallocation of base resources or a request for new funding. While the POAMs will not be used as agency funding requests by OMB, a brief rationale should be provided when a request for new funding is contemplated.

3) Management should create a separate cross-investment project for IT security. The IT security project should include all staff, in the form of full time equivalents (FTEs), assigned to IT security functions and all cross-investment contractor IT security support costs for each of the agency's IT investments.

4) Management should ensure that all relevant existing and future IT contracts include separate line items for security costs as the services and systems provided by contactors often include a security component.

5) Management should record the IT security costs documented in existing and future contracts across all investments in the capital planning and investment documentation. This will allow management to document both the in-house costs and the contractor costs and provide traceability to the capital planning and investment documentation.

6) Management should ensure that all project initiation requests include a line item for security. This line item will allow management to tie the security costs associated with the individual projects back to the investment and to the budgeting documentation.

7) Management should document the Unique Investment Identifiers (UII) associated with each security weakness in the agency POAMs and record the cost to remediate the weakness in the appropriate investment.

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 the CPSC management had not implemented sufficient operational controls in the area of personnel security, data integrity, and documentation, the CPSC management was not able to address security procedures to focus on security mechanisms that affect the daily operation of the Commission. OMB Circular A-130, Appendix III requires that sufficient operational controls for personnel security, data integrity, and documentation be in place. This condition may have been due to the CPSC management not having the resources necessary to make implementation of operational controls a priority. The level of risk was rated "high" for personnel security and data integrity.

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

Action Taken: Significant progress has been made since 2001 to address this issue, even though gaps remain. As previously mentioned, the CPSC developed the Information System Security Plan (SSP) for the GSS LAN in 2002. Patriot, the contractor that developed the SSP, reported that in order for the CPSC to adequately implement and maintain the requirements of the SSP, a staff of three full-time personnel (information system security officer, network security engineer, and applications security engineer) would be needed. Qualifications for and responsibilities of each position were delineated in the 2003 SSP. The CPSC has since hired an information system security officer and, in FY 11, provided him with one staff member to implement and maintain the SSP requirements. Management is also in the process of hiring a second information system security officer to oversee IT security. Management contracted out the remaining responsibilities on an “as needed” basis. However, management continues to require additional internal resources to adequately implement and maintain the SSP requirements.

In FY 2007, OMB mandated that agencies adopt security configurations for Windows XP and VISTA, as well as a policy for ensuring new acquisitions include common security configurations. (See OMB Memorandum M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," and OMB Memorandum M-07-18 "Ensuring New Acquisitions Include Common Security Configurations,") The CPSC has since formalized a Configuration Management Policy to govern this process. However, management had not fully implemented this policy, developed attendant procedures, or implemented configuration baselines for all agency hardware and software.

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.

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 10, FY 11 and FY 12 FISMA reviews, the OIG noted several improvements and new findings. Although the agency baselined Windows XP in FY 11, and implemented the United States Government Configuration Baseline (USGCB) [formally, the Federal Desktop Core Configuration (FDCC)] recommended configurations for Windows XP, management did not properly document or implement baseline configurations for all other agency software or hardware components. In FY 12, management baselined Windows 7 and the version of IE8 residing on the Windows 7 clients. However, management has not baselined the versions of IE7 and IE8 residing on the Windows XP clients. Management expects to decommission all Windows XP clients and to fully deploy Windows 7 no later than the first quarter of FY 13. Therefore, management does not intend to baseline this software.

Management also documented configuration baselines for the following software: Windows 2008, SUSE Linux servers, MySQL, Netware, Oracle, SQLServer, Sybase, and VMWare in FY 11. However, management has not reviewed or updated these baselines in FY 12. Management did not include all of the required information in these baseline documents. For example, management did not consistently document the current version of the software, the software's patch information, and the logical placement of the component within the system architecture. Additionally, management has not documented baseline configurations for any other system hardware or software, including the Windows Server 2003, Microsoft Office, SharePoint Server 2007, Checkpoint firewall, and Cisco IOS. Also important to note, management has not integrated updates to the baseline configuration documents into the change management process. Therefore, management does not capture changes to systems and system environments occurring throughout the year in the baseline document until the end of the year, at the earliest.

In FY 11, agency management began scanning agency clients for compliance with the required USGCB/FDCC settings. In FY 12, management began sharing a summary of these results in a monthly security status report. In addition, in FY 12, management selected the Defense Information System Agency (DISA) settings, available in checklist form in the National Vulnerability Database (NVD), to apply to agency systems to harden them. Management then began scanning agency software for compliance with these checklists. Although management has not applied these settings to all agency systems, they have begun to apply them to the Windows and Linux servers. Also in September 2012, management began to perform non-credentialed scans of the network to identify vulnerabilities. However, the agency has not developed and implemented a process to remediate the non-compliances identified in the USGCB/FDCC and DISA compliance scans or the vulnerabilities identified in the non-credentialed scans. Management also does not share the results of the DISA scans and the non-

credentialed scans with all of the appropriate agency officials to ensure they identify and eliminate similar vulnerabilities in other information systems (i.e., systematic weaknesses).

Management has not developed and implemented Standard Operating Procedures (SOPs) for the Configuration Management process. Management does not maintain a comprehensive inventory of hardware and software. Therefore, management does not have a comprehensive inventory of critical hardware and software requiring configuration baselines. Management has made some progress in remediating this issue and partially implemented tools to assist the agency in their efforts to develop and maintain a comprehensive software/hardware inventory. However, management has not selected all of the tools required to allow them to develop and maintain a comprehensive software/hardware inventory, and has not purged all known unauthorized software from the network. Furthermore, management did not adequately control local administrative access to clients throughout the entire year. This has increased the risk that users may installed unknown and unsecured software on the agency's network. However, in FY 12, management improved its controls over local administrator access to agency clients. Management limited the number of users with local administrative access to their clients and implemented a formal review of this access. With these improvements, management can ensure the agency only grants access to users requiring this access for their job functions. Although this improvement will not, in and of itself, remediate the issue, once management develops a comprehensive software inventory and implements a whitelisting solution, the agency will have substantially better control over what software and hardware resides on its network. These improvements will also assist the agency with its efforts to improve property accountability and software license compliance. Management cannot achieve software license compliance without these tools and controls in place.

As mentioned earlier, management does not adequately perform and document SIAs 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. Therefore, management cannot adequately perform an assessment to determine the security impact to the operating environment and control framework. Additionally, the ISSO did not approve all changes prior to implementation in FY 12.

The agency formalized a Change Management policy and Configuration Management Policy in FY 11. However, management has not fully implemented these policies. The Change Control Board does not approve all major configuration changes as required by the IT Change Control Policy and Configuration Management Policy. Management does not audit activities associated with system change control and management did not adequately document the testing procedures used to test all system changes. Therefore, system administrators may implement unauthorized or inadequately tested changes on the production network leaving the organization susceptible to unexpected system failures, as well as external and internal attacks.

The agency formalized a Patch Management policy in FY 11. However, management did not review and update the Patch Management policy in FY 12. Management has not implemented

an automated process to systematically identify flaws or vulnerabilities for all CPSC servers on a monthly basis. Management also does not report server flaws and vulnerabilities in the Monthly Security Status Reports. However, although management has not begun performing patch management scans on the agency's Linux servers, they began performing weekly patch management scans of the Windows Server 2003 and Windows Server 2008 servers on September 1, 2012.

Management has not implemented a process to require technical resources to identify and implement critical server, database and widely used application patches in a timely manner. Also, although management has implemented a process to patch agency clients in a timely manner, the resources responsible for these tasks did not consistently implement client patches in a timely manner. Management could not provided evidence that the agency tested server patches in accordance with NIST SP 800-53, SI-2 or the CPSC Patch Management Policy. Additionally, the language management included in the change management forms indicates that management deployed patches directly into production without being tested.

Configuration Management Recommendations:

1) Management should develop and implement SOPs to standardize the implementation of the Configuration Management process. The Configuration Management SOPs should include the following:

a) Time frames in which the agency must remediate / accept identified baseline variances.

b) The process by which management documents and justifies baseline configurations deviations (including USGCB/FDCC and DISA deviations)

c) The process by which agency resources coordinate and provide oversight for configuration change control activities. Agency resources must provide oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board] that convenes based on an organization-defined frequency and/or based on organization-defined configuration change conditions.

d) The process by which the agency reviews and updates the baseline configuration of each of the information systems. This process should include how frequently the agency reviews and updates the baseline configurations. It should also include a list of agency-defined circumstances requiring the update of the baselines. Additionally, it should outline how the agency updates the baseline configurations as an integral part of information system component installations and upgrades.

e) The process by which management identifies and inventories hardware and software requiring configuration baselines.

f) The process by which the agency identifies and justifies all systems and system components not requiring baselines. Currently, the policy refers to all "information systems". However, management does not intend to baseline all information systems. Instead, the agency plans to determine the systems that require baselines and develop the configuration baselines accordingly.

g) What information management must include in each configuration baseline SOP (e.g., configuration settings, patch level, Software Load and Version, system architecture, where the resource resides on the network, etc.).

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. Business owners should identify Mission Essential Functions and systems and provide this information 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. These configuration settings should use defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

4) Management should then implement the identified configuration settings.

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

6) Management should then monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

7) The agency should implement a solution to develop and maintain a current and comprehensive software/hardware inventory. Management can install agents on all CPSC machines to allow the agency to utilize Simple Network Management Protocol (SNMP) to develop a hardware inventory. However, this approach includes known security risks. Therefore, if management chooses to address this finding by implementing SNMP, management should perform an assessment of the risks posed by SNMP.

8) Management should purge the network of all unauthorized software.

9) Management should implement a whitelisting tool that will systematically prevent unauthorized software from running on the network.

10) Management should perform and document Security Impact Analyses for each system changes that include a sufficient level of detail to allow the CPSC security team to make a determination of a system change's impact to the agency's control environment.

11) Monthly security status reports, developed to describe the results of the ongoing continuous monitoring activities performed by the agency, should include the results of the Security Impact Analyses. At minimum, the security status reports should describe or summarize the results of the SIAs, key changes to SSPs, SARs, and POA&M's, and the results of the scans described in the Continuous Monitoring Plan.

12) Management should develop a comprehensive Enterprise Architecture and management should tie all system changes to the EA.

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

14) Management should actively maintain and update all baseline configuration documents. Management should update baseline configuration documents anytime a change is implemented that has an impact on the baseline configurations.

15) Management should develop a process to remediate non-compliances to the baseline configurations identified as part of monthly scans, and document that process in an SOP.

a). Management should include a requirement to document a remediation plan for all non-compliances identified as part of the monthly configuration management scans in the Configuration Management Policy (or related SOPs).

b). Management should document required timeframes for the remediation of non-compliances identified as part of the monthly configuration management scans in the Configuration Management Policy (or related SOPs).

16) Management should implement the process outlined in recommendation 15, and ensure that the agency remediates configuration baseline non-compliances in a timely manner.

17) Management should also implement and document controls to mitigate the risk posed by the accepted variances to the configuration baselines.

18) Management should include a summary of the results of the DISA configuration compliance scans in the monthly Security Status Reports.

19) Management should include a summary of the results of the non-credentialed vulnerability scans in the monthly Security Status Reports.

20) Management should provide detailed results from configuration management and vulnerability scans to each of the branch chiefs to allow for the identification of systematic weaknesses/deficiencies.

21) A Change Control Board should approve all major configuration changes.

22) Management should update the baseline configuration documents, as appropriate, to reflect any changes resulting from the configuration changes and patches.

23) Management should audit production changes periodically to validate the agency has adequately tested, documented and approved them.

24) The ISSO or delegate should approve all system changes.

25) Management should provide training to resources responsible for implementing system and configuration changes. Management should train these resources on the CPSC change management procedures, and what information management requires when documenting a configuration change in a change management form.

26) Assign a resource to act as a backup to the resource responsible for the patch management process to ensure management applies patches in a timely manner.

27) Management should follow the processes outlined in the Patch Management Policy to ensure timely testing and application of all server patches.

28) Management should implement an automated process to systematically identify flaws and implement patches for all CPSC servers.

29) Management should implement server, database, and widely used application patches in a timely manner and in accordance with the patch management policy.

30) Management should test all server, database, and application patches in a test environment prior to deploying the patch to production.

31) Management should document all server, database, and application patches in the change management database and document the process used to test these patches.

32) Management should add separate queries to the change management database to allow users to search on server, database, and application patches.

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

34) Management should improve the process for managing the IT software requests. Management should implement an automated tool (such as SharePoint) that houses all of the IT software request information and software licensing information. Management should use this tool to obtain and document software requests. Management should also use this tool to systematically require approval by the appropriate resources prior to closing / completing the new software request.

35) Management should develop and enforce a process to govern software license compliance:

a) Management should document and maintain a comprehensive software inventory.

b) Management should document the number of instances of each type of software installed on the network.

c) Management should document and inventory all software licenses owned by the agency.

d) Management should reconcile the software instances installed on the network to the software licenses owned by the CPSC and remediate any discrepancies.

e) Management should perform periodic audits to ensure compliance.

Incident Response and Reporting review:

The agency developed and formalized an Incident Response Policy on August 20, 2011 and management reviewed and updated this policy on August 6, 2012. Additionally, management developed an Incident Reporting database, to track incident reports, and this tool resides on the IT Security SharePoint site. Management also maintains the existing Incident Response policy, procedures, and plan in the IT Security SharePoint site. However, management has not finalized the procedures or fully implemented the policy.

Management has assigned resources to a Computer Security Incident Response Team (CSIRT). However, management has not trained these resources on their incident reporting responsibilities, and these resources are not performing the tasks outlined in the policy and procedures. Until this process is established and operational, management cannot adequately perform a comprehensive analysis of, validate, and document all security incidents.

Currently, the CPSC security team documents and tracks all security incidents of which they are notified in the Incident Response Database. The documented security incidents include the date the incident began, a description of the incident, the priority of the incident, comments from incident handlers, the status of incident, and the next steps taken. However, the OIG could not attest to the timeliness of the security team's response to and resolution of security incidents because management did not include enough detail in the incident documentation. The incident reports do not include the time and date of security team notification, and the incident response policies, procedures and plan do not outline performance metrics, such as response times, days to resolve, and out of tolerance indicators. Therefore, the OIG could not assess if the security team responded to and resolved incidents in a timely manner. However, the OIG found several documented security incidents that remained active and unresolved despite management having opened them between 2 and 20 months ago.

The agency drafted Forensic Incident Response procedures and an SOP that outlines law enforcement notification requirements in FY 12. However, management does not intend to implement these procedures until FY 13. Additionally, management did not notify United States Computer Response Readiness Team (US-CERT) in accordance with the timeframes outlined in the Incident Response Policy and in the Federal Guidelines for the documented incidents.

Additionally, management implemented several solutions since FY 11 to improve its ability to monitor for incidents. Management partially implemented the Trusted Internet Connection (TIC) in July of 2012 and a log management solution in FY 11. The TIC consolidates external network connections across the Federal government. The TIC also allows for the central monitoring of network traffic for malicious activity, across the government. A monitoring tool called Einstein 2 that management implemented in conjunction with the TIC facilitates this. The Einstein 2 solution monitors for specific predefined signatures of known malicious activity at the agencies Internet connections. Einstein 2 alerts US-CERT directly when it detects specific malicious network activity matching predetermined signatures allowing the CPSC to utilize US-CERT expertise and resources.

Management implemented and configured a log management solution to notify system administrators of a list of predefined security events identified by other network monitoring solutions. Management has not yet fully optimized the log management solution, although management has made significant progress in this effort. For example, the log management solution now notifies management of the occurrence of predefined events across eight different monitoring tools. However, management has not implemented a solution to monitor for actions constituting internal threats or to identify unauthorized activity by inspecting outbound network traffic (extrusion detection). Although management maintains VPN and Firewall logs, management does not actively monitor these logs due to a lack of resources to perform these tasks. The log management solution is capable of such monitoring. However, at this time management has not configured the log management solution to alert management on predefined VPN traffic activities, and the only firewall activity the log management solution reports on are changes to firewall policies.

Incident Response and Reporting Recommendations:

1) Management should define performance metrics, such as response times, days to resolve, and out of tolerance indicators, in the policies and procedures based on best practices and industry standards and adjust them once the incident response process evolves.

2) Management should fully implement the Incident Response policy and procedures.

3) Management should train the CSIRT members on the responsibilities assigned to each of them and implement the CSIRT in accordance with the Incident Response Plan.

4) Management should implement and configure an extrusion detection solution to alert administrators of potential internal treats.

5) Management should implement a solution and configure it to alert management in the event of an organization defined list of VPN or firewall events, such as suspicious outbound traffic, or suspicious activity on an unusual port. This will allow for a meaningful analysis of both internal and external network activity. Alternatively, management should formally perform a manual review the VPN/firewall logs to identify suspicious activity and correlate these events.

6) Management should notify US-CERT and law enforcement of security incidents within the federally and organizationally prescribed timeframes.

7) Management should report all security incidents to the ISSO immediately upon discovery, and the ISSO should track these incidents in the Incident Response Database. Incidents tracked should include relevant alerts from monitoring tools, as well as VPN and Firewall alerts (based on an organization-defined set of criteria).

8) Management should not only date-stamp but also time-stamp all actions taken to address security issues in the incident response reports.

9) Management should document the time and date the security team/CSIRT is first notified of the incident in the SharePoint tool used to monitor the incidents.

Security Training:

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

Management's increased efforts to ensure CPSC personnel complete the agency provided security awareness training have resulted in substantial improvements. In FY 12, management implemented a zero tolerance approach for addressing personnel who did not complete their annual security awareness training. Management now revokes access to any user who does not complete the CPSC provided security awareness training course within the provided timeframes. Implementing this approach has increased security awareness training participation from 67.5% in FY 11 to 96% in FY 12.

Security Training Recommendations:

1) The agency should develop a NIST SP 800-16 compliant training program.
   a) The Security Awareness and Training policies and procedures should require management to provide each NIST SP 800-16 "user group" defined within the agency security training program, role based training specifically developed for their group.
   b) The training criteria, if not the content, for each user group should be outlined in the policy. For details on the required training criteria, please see NIST SP 800-16, pages 98 - 154; NIST SP 800-16, appendix E; and summaries in NIST SP 800-50, pages 25-27.

2) Agency management should assign all agency resources to one of the 25 user groups documented in NIST SP 800-16.

3) Once assigned to a NIST SP 800-16 defined user group, agency management should then select appropriate training courses and provide security training to those agency resources commensurate with their user groups. The DHS Information System Security Line of Business (ISSLOB) has been working with agencies to develop a standardized curriculum and to select information security Shared Service Centers (SSC). The ISSLOB SSC's provide an efficient and cost-effective solution for agencies to procure general information security training for employees and contractors. For more information on this program, contact the ISSLOB program management office at isslob@dhs.gov.

3. Security Technical Controls

Prior Finding: Security technical controls are specific to the system's ability to identify, track, and act on authorized or unauthorized usage. Because the CPSC management had not implemented sufficient technical controls in the areas of identification and authentication, logical access, and audit trails, the CPSC management had left sensitive information vulnerable. This condition appears to have been due to the 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: The CPSC management should implement sufficient technical controls in the areas of identification and authentication, logical access, and audit trails in order to protect the information that is used to support the mission of the Commission.

Action Taken: The effectiveness of six of the CPSC's systems, and the underlying elements of each, were tested during the FY 2001 audit. Weaknesses identified in controls related to these systems contributed to the overall condition of the CPSC's information security program. As reported in the management response to the original audit, the CPSC requested funding in Fiscal years 1999 through 2002 without success to establish a capital budget for information technology. The need for such funds was also included, unsuccessfully, in the CPSC's FY 03 and 04 budget requests. Budget requests cited the need for new investments to protect the current operating capability and efficiency of information technology. According to the Budget Officer, in the absence of a capital budget for information technology, the CPSC has applied some savings from operating funds to this area. In FY 02, the CPSC committed over $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 03, the total CPSC Information Technology commitment was $714,891 in the form of salaries and other expenses. In FY 04, the CPSC committed $715,000 for its Information Technology programs. In FY 05, this figure rose to $1,035,100. In FY 06, the CPSC spent $2,082,050 on its IT programs. In FY 07, the CPSC committed $6,300,000 to its IT program. In FY 08, the CPSC's commitment rose to 30 FTEs and $13,000,000. In FY 09, the CPSC's commitment rose to 31.1 FTEs and $19,832,939. In FY 10, the CPSC's commitment rose again to $26,492,137. However, in FY 10 the FTEs fell to 30.9. In FY 11, the CPSC's commitment fell to $23,617,310. However, FTEs increased from 30.9 in FY 10 to 36.6 in FY 11. In FY 12, the CPSC's expenditures committed to IT services fell again to $21,617,065 and FTEs decreased to 36.4. Work on implementing the recommendations contained in the SSPs 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, implementing solutions to perform automated system auditing, implementing the monitoring of Internet usage, implementing an Intrusion Prevention System, implementing multi-factor authentication for most agency resources, implementing a solution to restrict access to client USB ports by non-encrypted flash drives, implementing periodic reviews of user with elevated network privileges, and implementing a tool which allows the agency to inventory all network user accounts.

Remote Access Management review:

Management developed and formalized policies for authorizing, monitoring, and controlling remote access in FY 11, and management updated and recertified these policies in FY 12. However, the Remote Access Management policies do not include several key elements. The Remote Access Management policy does not include a list of security functions and security-related information that users can access remotely or the additional controls management has implemented to ensure these users do not misuse this access. Additionally, management has not defined the networking protocols the agency has deemed non-secure within the policies/procedures.

Although management has developed Teleworking and Remote Access procedures, these procedures do not address several operational topics. The procedures do not provide for checking for upgrades and patches to the remote access software components, and acquiring, testing, and deploying those updates. The procedures do not address reconfiguring access control features as needed based on factors such as: policy changes, technology changes, audit findings, and new security needs. Moreover, the procedures do not address detecting and documenting anomalies identified within the remote access infrastructure. Such anomalies might indicate malicious activity or deviations from policy and procedures. These anomalies should be reported to other systems' administrators as appropriate. Furthermore, procedures in place for monitoring remote access are inadequate. Management has not implemented controls, such as ingress filtering, egress filtering, deep packet reviews, non-repudiation controls, or VPN and firewall logs reviews, to detect and prevent the subversion of authorized connections. Management has attributed this to current system limitations making the active monitoring of these logs impractical and to an overall lack of resources.

Additionally, management has not fully implemented the remote access policies and procedures. The Remote Access Policy states that remote sessions time-out after 30 minutes of inactivity. However, management has configured these sessions 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. Management also does not monitor or review VPN and firewall logs as is required by the Remote Access policy. The agency also has a policy, which requires users to encrypt all sensitive information prior to transmitting the information outside of the internal network. However, although the agency has implemented a tool to facilitate compliance with this requirement in FY 12, management has not configured the CPSC email solution to systematically encrypt emails prior to transmission across a public network. Also, management does not perform audits to ensure all sensitive emails and attachments transmitted across a public network utilize the encryption tool appropriately. Therefore, although the process has improved with the implementation of the encryption tool, an extremely high likelihood remains that users send unencrypted, sensitive files over Public networks.

Management does not require all users to use multi-factor authentication to access the network. Although management has not fully satisfied the NIST SP 800-46 and OMB M07-16 requirements, management has made substantial progress toward that goal and only a limited number of users remain who can access the network without the use of their Personal Identification Verification (PIV) Card. Management does not uniquely identify and authenticate

users accessing the network. Management has not implemented a formal process to control the establishment and maintenance of common E-Directory and Active Directory (AD) accounts. Additionally, management does not change account credentials when users separate from the agency or change job functions. Moreover, the Network Engineering and Computer Support Teams use generic administrator IDs to perform support functions. Agency resources that have administrative rights access the GSS remotely using administrator accounts. Furthermore, management does not monitor the tasks performed by the administrators while using these IDs.

Management does not properly document and report lost or stolen laptops/blackberries. Management did not document all of the laptops and blackberries lost in FY 12 in the Incident Reporting database. Management also did not report all of these lost devices to US-CERT. In addition, management does not document the time the user reports the lost/stolen device. Therefore, management cannot document the timeliness of its notification to US-CERT for these types of events.

Remote Access Management Recommendations:

1) Management should document and implement the following processes in a procedure document:

a) A list of the security functions and security-related information that users can access remotely and the additional controls in place to ensure these functions are not misused. In addition, management should implement and document specific audit procedures to ensure these controls are in place and effective.

b) An inventory of networking protocols management deems non-secure and a requirement to restrict access to these protocols.

c) The process by which management checks for upgrades and patches to the remote access software components, and acquiring, testing, and deploying the updates.

d) The process by which management reconfigures access control features based on factors such as policy changes, technology changes, audit findings, and new security needs.

e) The process by which management detects and documents anomalies 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

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

3) Management should implement a solution to systematically require the encryption of all sensitive information transmitted across a public network. Or periodically audit emails and attachments traversing a public network to ensure policy compliance. Or implement a data loss prevention (DLP) solution.

4) Management should implement the CSIRT Team and assign them the task of documenting and remediating the risks associated with missing and stolen laptops and blackberries.

5) Management should systematically require multi-factor authentication for all users accessing the CPSC network.

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

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

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

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

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

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

12) Management should actively monitor remote user access and implement controls to detect and prevent the subversion of authorized network connections. Management may achieve this by the implementation of procedures and tools to facilitate ingress filtering, egress filtering, deep packet reviews, and VPN and firewall log reviews. Additionally, management should report the results of these analyses and all other appropriate parties.

Identity and Access Management review:

The agency formalized the General Access Control policy on August 10, 2011 and recertified the policy with updates on September 10, 2012. However, the procedures outlined in the General Access Control policy did not include several key elements. These procedures did not include: the process by which management establishes and controls common/shared network accounts; the process by which management establishes and controls temporary, emergency, and guest accounts; the process by which management establishes and controls system accounts; and account modification procedures. Management did not reference the individual system access control SOPs for the agency's major applications in the General Access Policy. Management also has not finalized an Access Control Policy and attendant procedures for CPSRMS.

Although management formalized the General Access Control Policy, management has not fully implemented the policy. The General Access Control Policy requires that agency management audit all users with access to the CPSC systems and confirm the accuracy of the group access settings. Management is also required to submit the results of these audits to the ISSO for record and maintenance purposes. However, management does not perform this audit.

Also, although management began performing periodic user access reviews on a semi-annual basis in FY 12 for many agency systems, management did not perform a periodic user access review for the CPSRMS application in FY 12.

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 that it expects to remediate this issue. Management hopes to implement this solution in FY 13.

Management does not require all CPSC users to access the network using multifactor authentication. However, management has made significant progress in implementing this requirement. Management has configured all Window 7 clients to require multifactor authentication and management plans to migrate all agency users to Windows 7 by the first quarter of FY 13. Once management completes the Windows 7 migration, network administrators will be the only users able to access the network without multifactor authentication. Management has decided to accept the risk associated with this vulnerability.

The agency has not implemented the Principle of Least Privilege and proper separation of duties for the GSS LAN. The agency does not have the ability to report on users with access to specific security functions within AD or E-Directory. Because the agency has not implemented a solution that will allow them to develop reports with this level of granularity management cannot apply the Principle of Least Privilege. Management has only configured 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. In addition, users with administrative rights have the ability to access the GSS remotely using their administrator accounts. Management does not require separate accounts for these users to telework or perform non-administrative tasks. In addition, the agency has not implemented the Principle of Least Privilege for CPSRMS. All CPS360 (a module within CPSRMS) users can view all incident reports, even those that management has not approved for Public consumption, whether or not their job function requires access to these data views.

Management began performing weekly staffing report reviews in FY 12 to ensure that the agency revoked separating employee's access to the network in a timely manner. However, management does not perform this reconciliation for all agency systems. The OIG also noted that, even with the improvement to the process, management does not consistently disable access to the agency network or other information systems immediately upon employee and contractor separation. The OIG identified separated employees and contractors whom management had not revoked from agency information systems as of September 30, 2012. In addition, management does not record the time and date it disables user accounts, and cannot provide evidence of the timeliness of these revocations.

The OIG also noted management has not implemented an effective process for tracking and inventorying CPSC contractors. The contractor inventory and separation reports contain

inaccuracies. Active contractors appear on the contractor separation reports, and do not appear in the contractor inventory reports. The contractor inventory process is a manual process that requires coordination between EXRM, EXIT, and agency Contracting Officer's Technical Representatives (COTRs). Management has not developed and does not actively maintain a centralized contractor database to track contractor on-boarding and off-boarding. This, in addition to the lack of process standardization, has limited management's ability to revoke the information system access for separating contractors in a timely manner.

Management implemented a process to perform semi-annual reviews of major application user accounts in FY 12, although management did not perform this review for CPSRMS. Management also implemented a process to perform a semi-annual review of common user accounts with elevated privileges in FY 12 and eliminated unnecessary common accounts. However, management has not defined a formal process to establish and further control shared/common user accounts. Management does not change credentials related to common/shared accounts once resources separate from the agency or change job functions. Additionally, and compounding this risk, is management's use of generic administrator IDs.

Identity and Access Management Recommendations:

1) Management should update the General Access Control policy to include roles and responsibilities and to document how management coordinates access control tasks between the CPSC branches.

2) Management should include the following elements in the General Access Control Policy and procedure documents:

a) The process by which management establishes and controls common network accounts. This should include how management authorizes and monitors common/anonymous accounts.

b) The process by which management establishes and controls temporary, emergency and guest accounts. This should include guidance on how management authorizes and monitors guest/temporary accounts. The procedures should define process for notifying account managers when temporary accounts are no longer required. The procedures should also include a requirement to deactivate temporary accounts that management no longer requires access to them.

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

d). The 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). The General Access Policy should reference the individual system access control SOPs.

3). Management should draft, approve, and implement NIST compliant Access Control policies and procedures for CPSRMS.

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

5). Management should ensure the distribution of Access Control policies and procedures to all resources with significant access control roles and responsibilities.

6). Management should create separate non-administrative user accounts for administrators, and require administrators to use these accounts when performing tasks that do not require administrative privileges.

7). Management should implement a solution that uniquely identifies and authenticates devices prior to establishing a connection to the CPSC GSS.

8). Management should systematically require all users accessing the CPSC network to utilize multi-factor authentication.

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

10). Management should implement the Principle of Least Privilege for 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, modify DHCP, etc.)

b). The agency should revoke access to all users who have but do not require access to the functions defined above.

c). The agency should review the logs of all admin/super user accounts and restrict this access if these levels of privilege are not specifically necessary to perform required job functions.

d). The agency should document the system controls in place (e.g., blocked ports, restricted protocols, etc.).

e). The agency should document the specific access controls in place for providing/controlling access required for the duties, functions and system restrictions described above. Documentation can be in the form of access control policies (e.g., identity-based policies, role-based policies, attribute-based policies, etc.).

f). Management should require administrators to utilize a non-administrative user account to perform tasks which do not necessitate the use an administrator account.

11). Management should implement a solution that allows the agency to report on the specific privileges assigned to each AD and E-Directory user account. These reports should be granular enough to report on which security function management assigns to each user account. Management should perform periodic audits of these reports to ensure access remains appropriate.

12). Management should limit administrator's access to update audit logs and implement a solution to monitor changes to the audit logs and notify the CSIRT team in the event of an audit log modification.

12). Management should implement a solution to actively monitor tasks performed by resources with approved conflicting duties.

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

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

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

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

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

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

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

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

14). Management should revoke the separated user's access to E-Directory, AD and CPSRMS.

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

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

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

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

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

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

MANAGEMENT SUMMARIZED RESPONSE

After having been given an opportunity to review a draft copy of the report, and having already had ample opportunity to review the individual findings that comprise the report, management concurred with the findings and recommendations.

Management elected to not provide a formal written response, other than preparing a transmittal letter, bearing the signature of the head of the agency, to be used by them to forward this report to the Office of Management and Budget which stated, "I have reviewed the FISMA report and agree with the Inspector General's assessment. Our plan to remediate any outstanding issues will be reflected in our quarterly Plan of Action and Milestones report."