

U.S. CONSUMER PRODUCT SAFETY COMMISSION



OFFICE OF THE INSPECTOR GENERAL

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT

REPORT

Issued: November 15, 2010

Reformatted: November 30, 2010



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
WASHINGTON, DC 20207

Memorandum

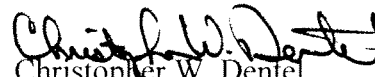
Date: November 30, 2010

TO : Chairman Inez M. Tenenbaum
Consumer Product Safety Commission

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Federal Information Security Management Act Audit (FISMA)

This year's FISMA evaluation found that although much work has been done much work remains to be done. For example, 81 findings (15 of which are high risk issues) were noted in this year's review. 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 and the implementation of the public facing database (CPSRMS).¹


Christopher W. Dentel
Inspector General

¹ The CPSIA requires the development of a database of publicly available information on incidents involving injury or death required under section 6A of the Consumer Product Safety Act and the integration of the database into the Commission's overall information technology improvement objectives and plans.

Federal Information Security Management Act Report
Table of Contents

	Page
EXECUTIVE SUMMARY	1
Office of the Inspector General's Results	
INTRODUCTION	3
Background	3
Objective	4
Scope and Methodology	4
RESULTS OF EVALUATION	5
Prior Findings, Recommendations, and Actions Taken	
Security Management Controls	5
Security Operation Controls	13
Security Technical Controls	20
Performance Measures	27

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

FEDERAL INFORMATION SECURITY 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 CPSC's automated information security control procedures and practices in Fiscal Year 2001. The audit included tests of entity-wide controls and six of CPSC's 49 application systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology Special Publication (SP) 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 IG's Fiscal Year 2010 evaluation. This review was completed in accordance with the Quality Standards for Inspections issued by the Council of Inspectors General on Integrity and Efficiency's (CIGIE) Inspection and Evaluation Committee and not the Generally Accepted Government Audit Standards issued by the Government Accountability Office.

This year's FISMA evaluation found that although much work has been done much work remains to be done. For example, 81 findings (15 of which are high risk issues) were noted 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 and the implementation of the public facing database (CPSRMS).

In addition to the findings made by the OIG and outlined in the FISMA review, several other weaknesses, many of which are high risk (35 High Risk), were noted by CPSC management as a result of the FY 10 Security Test and Evaluation Plan (ST&E), Risk Assessment and the development of the System Security Plan (SSP). The general theme ensuing from the results of the reviews tended to be 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 being enforced throughout the fiscal year and a lack of adequate tools to facilitate the required system reporting. However, although many of the policies have been updated and several of the procedures have been made more effective; many more

improvements are still required, as noted below. Additionally, several new software tools (ex. BigFix, Zenworks, Novell Sentinel, Einstein2, etc.) are being researched to determine if they can be used to improve system monitoring and reporting.

A number of remediation strategies are already being considered by the CPSC to address known vulnerabilities. The highest risk vulnerabilities are receiving first priority in the remediation process. However, the CPSC is in the early phases of remediation and the full mitigation of these risks will require a significant amount of additional effort. For example, one of the high risk vulnerabilities noted was the lack of baseline security configurations. The CPSC is taking steps to ensure the issue is remediated such as: researching tools to catalog software on the network, facilitate the identification of known configuration vulnerabilities and log variances to established baselines; however, many additional steps will be required before a true configuration baseline can be developed and configuration change management process can be enforced.

Another example of remediation activities undertaken by CPSC management to eliminate existing vulnerabilities and improve overall system security is the proposed implementation of a Continuous Monitoring Plan, developed by SecureIT on August 27, 2010. The implementation of this plan will result in several vulnerabilities being remediated simply due to the improvements required in system reporting to facilitate the new Continuous Monitoring strategy. The improvement in the reporting and analysis, which will be possible as a consequence of the enhanced reporting, will allow issues in other processes such as Remote Access governance, Identity Management, Security Awareness Training and Security Incident Reporting to be identified, quantified and remediated much more efficiently and effectively than is currently possible. This, in addition to the harmonizing of processes required for this reporting, will be 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 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) contracted with Grant Thornton to perform an independent audit of CPSC's automated information security control procedures and practices in FY 2001. The requirements of the audit included:

- Evaluating and testing the internal controls, evaluating weaknesses and identifying the degree of risk for the related weakness.
- Testing the effectiveness of the information security controls on a sample of CPSC's systems.
- Assessing whether CPSC's information security policy, procedures, and practices comply with Federal laws, regulations, and policies.
- Recommending improvements, where necessary, in security record keeping, internal security controls, and system security.
- Identifying the degree of risk associated with identified internal security controls weaknesses.

The audit included tests of entity-wide controls and six of CPSC's 49 applications systems and their underlying elements. Grant Thornton used the National Institute of Standards and Technology Special Publication (SP) 800-XX, Draft Self-Assessment Guide for information Technology Systems, March 9, 2001 to test security controls. The objective of the audit was to determine whether CPSC's automated information system was adequately safeguarded.

In its report, Audit of Automated Information System Security, Grant Thornton, identified material weaknesses in CPSC's management, operational, and technical controls policies, procedures, and practices. According to the report, the conditions of these controls could permit the modification or destruction of data, disclosure of sensitive information, or denial of services to the users who require the information to support the mission of the CPSC. In addition, it was

reported that the CPSC did not have a capital budget for IT security. Without appropriate capital budget planning, Grant Thornton was concerned that CPSC's management might not be able to properly implement and maintain resources to ensure system safeguards.

Furthermore, to ensure proper coverage and mitigation of the risks identified by the OMB, the CPSC performed its own testing procedures to assess the design and implementation of the OMB defined FISMA requirements (please see the Scope and Methodology for additional details). Additionally, the CPSC OIG reviewed the 2010 Risk Assessment, Hardware and Software Inventory Report, ST&E (Security Test and Evaluation Plan), SAR (Security Assessment Report) and SSP (System Security Plan) which were developed by SecureIT (the IT consultancy contracted by EXIT) to update its understanding of the current processes and procedures employed by the CPSC. However, since the OIG did not directly contract with SecureIT and their testing was limited to the design of the NIST 800-53 controls and not to their operating effectiveness, the OIG placed only limited reliance on this work.

The scope of the ST&E and SAR encompassed the entire CPSC GSS (General Support System) as defined by the GSS boundary outlined in the Hardware and Software inventory report. The scope also included all associated policies, procedures, processes and documentation that is used and maintained in the operation and maintenance of the CPSC GSS.

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

Scope and Methodology: The evaluation was conducted from August to October of 2010. This evaluation consisted of a review of the following FISMA defined agency processes within the boundaries of the GSS LAN as defined by the SecureIT in the Hardware and Software Inventory Report dated June 30, 2010:

- Certification and Accreditation
- Security Configuration Management
- Security Incident Management
- Security Training
- The Plan of Actions and Milestones (POAM)
- Remote Access governance;
- Identity Management;
- Continuous Monitoring
- Contingency Planning
- Contractor Oversight

This review constitutes 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 defined by FISMA. However, this year's review does not consider the status of the CPSC Data Privacy Program, as this process was not defined as an in-scope process this year by the OMB.

The status of each of these items was 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 CPSC officials and contractor personnel was reviewed as necessary.

RESULTS OF EVALUATION

Prior Findings, Recommendations and Actions Taken: The FY 2001 audit of CPSC's information security program revealed several material weaknesses in CPSC's security policies, procedures, and practices. Specifically, CPSC management had not implemented sufficient management, operational, and technical controls. All previously identified material weaknesses have now been corrected. No additional material weaknesses have been identified. However, due to a combination of budget limitations and the new security system requirements promulgated by NIST and OMB, the CPSC 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 address management were not fully implemented. OMB Circular A-130, Appendix III requires sufficient management controls in these areas. This condition appears to have been due to CPSC management not having the resources necessary to make the implementation of Security Management controls a priority.

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

Actions Taken: CPSC contracted with Patriot Technologies (Patriot) to develop an Information System Security Plan (SSP), January 31, 2002, that conforms to OMB Circular A 130 requirements and responds to Grant Thornton's findings. The new SSP provides CPSC with an overall security plan describing a functional information systems security framework. It describes CPSC organizational responsibilities for information system security.

In FY 03, CPSC contracted with PEC Solutions Inc. (PEC) to perform systems certification and accreditation and to develop a plan to ensure adequate management control in the areas of risk management, review of security controls, life cycle management, authorized processing, and system planning. In addition to the SSP, a System Development Life Cycle (SDLC) Plan and Business Continuity Plan were prepared. PEC successfully completed the work contracted for

regarding system certification and accreditation, risk management, and the development of a SDLC Plan and a Business Continuity Plan. All previously identified "material weaknesses" in these areas were addressed. Although PEC did not find that "full" certification and accreditation of CPSC's systems was appropriate in FY 03, they did issue an "interim approval" and indicated that full certification would be appropriate once certain recommendations set out in their report were achieved.

In FY 04, after those deficiencies that were found to be "material weaknesses" were addressed, the CPSC began the process of implementing the recommendation set out in these plans to deal with more serious security deficiencies ("high" priority security vulnerabilities). Ten of the eleven "high" priority security vulnerabilities were mitigated. The eleventh, after a new cost risk analysis was completed, was reclassified as an "acceptable risk." As a result of the work done in FY 04, the interim label was removed from the CPSC's system certification and accreditation.

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

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

In order to both meet the accreditation and certifications requirements outlined above and to determine whether the security controls identified for the CPSC Network General Support System in the System Security Plan were implemented correctly and effectively, in 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 Network General Support System. Of these, six were found to be high risk vulnerabilities, 31 were found to be medium risk vulnerabilities, and 26 were found to be low risk vulnerabilities. The STE Evaluation Report included a planned mitigation with an associated due date for each vulnerability identified.

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

In FY 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 changes in 2009 have been made to help the agency address this shortcoming, the POAM has not historically been used by the CPSC as an affirmative management tool in addressing security weaknesses. Although it has historically done a good job of documenting known security weaknesses and prioritizing

them, the agency has not used the 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 lacks historical data regarding its past efforts and fails to take advantage of a powerful planning tool in addressing current and future IT security challenges. Moreover, as of the conclusion of FY FISMA 10 review, the POAM still had not been adequately implemented.

Our FY 09 review determined that the CPSC IT System had maintained its certification and accreditation and that the system's security controls, in the opinion of management, had been tested and reviewed in so far as the agency continuously monitored the system. However, the Contingency Plan had, again, not been tested within 2009. Although this issue is not sufficient to cause the CPSC to lose its system accreditation, it continues to be troubling.

The CPSC SSP states that the security program shall provide for a review of the technical security controls at least once every 3 years. OMB Circular A-130, Appendix 3 (section A.3. 3) states that security controls should be reviewed in each system when significant modifications are made to the system but at least every 3 years. The risk assessment which was relied upon in FY09 was completed in 2006 and was over three years old at the time of reliance. The CPSC had not begun the process of reassessing security controls over its IT system in FY09, possibly because of the impending major changes to the system required by the implementation of the Consumer Product Safety Improvement Act.

Because no review had been documented, the agency could not show that FY09 security risks and vulnerabilities had been remedied and/or what new security risks and vulnerabilities might have existed. The CPSC should perform and document a formal review of its technical security controls on a regular basis.

In FY 10, EXIT contracted with SecureIT to perform the annual Risk Assessment, ST&E, SAR, develop the SSP (formerly referred to as the ISSP) and define a Continuous Monitoring process. This has allowed the CPSC to identify risks, define compensating controls and outline remediation actions. As a result of the ST&E / SAR exercise several major weaknesses were identified. For example, the control assessment portion of the SAR reported 147 (~56%) of a total of 261 applicable NIST 800-53 controls were not satisfied; the Security Vulnerability portion of the SAR reported a total of 3164 vulnerabilities (1212 are considered high severity vulnerabilities, 571 are considered medium severity vulnerabilities and 1381 are considered low severity vulnerabilities) across a sample of 35 hosts (resulting from inconsistent / inadequate patching) and the Baseline Configuration section of the SAR reported 3063 (~51%) failed compliance checks from a total population of 6018 across 19 devices. In addition to reporting the weaknesses, the SAR included recommendations to CPSC Management for how to mitigate the risks associated with individual control deficiencies identified in the SAR as well as proposed process improvements.

FY 10 POAM Review

As a result of the OIG's follow up on actions taken to remediate prior findings and the testing for the FY 10 FISMA review several new findings were noted. The POAM was not formalized until November 10, 2010, therefore the OIG cannot attest to its effectiveness (ex. timeliness of

the completion of remediation activities, accuracy of the scheduling estimates and timely updating of the POAM, adequate POAM updating/reporting). Additionally, the Certification and Accreditation (C&A) Policy (and attendant procedures) which defines the POAM process and outlines how known IT vulnerabilities / weaknesses are to be tracked, prioritized and remediated was not formalized and approved until September 9, 2010 and has not been fully implemented.

The C&A policy requires the definition of the weaknesses based on the SSP, SAR and other sources; tasks required to remediate the identified vulnerability; resources required for each task, scheduled completion date; prioritization strategy (based on the annual Risk Assessments); source of the identification of the vulnerability and the status of the remediation activity and although, the policy does not explicitly outline all OMB required POAM components (ex. defining a CPSC Point Of Contact, estimated costs, the tracking of changes to milestone dates, milestone deliverables, etc.), the policy reads “The CISO/ISSO must develop specific Plans of action and milestones (POAM) based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations” which implies they are required. However, the attendant procedures have not been fully implemented. For example, no systematic process is in place to determine how much a particular remediation activity will cost, how long the activity will take or how many resources the activity will require. Additionally, program officials and contractors do not report progress on remediation activities to CPSC management on a regular basis. Moreover, because the POAM process has not been fully implemented, the CPSC have not provided system authorizing officials with security status reports covering updates to POAM additions. Furthermore, the System Security Plan which include the results from the Risk assessments and Security Assessment Reports prior to this year had not been provided to the Authorizing Officials for his review and was not this year until November 9, 2010. Additionally, the CIO did not centrally track, maintain, and independently review/validate the POAM and the status of associated remediation activities on a quarterly basis until November 10, 2010. Therefore, only the November POAM review could be substantiated through documentation for FY 10.

FY 10 POAM Recommendations:

- 1) Update the C&A policy to explicitly include the following items:
 - a) Mapping from the POAM to the source document
 - b) The logging/justification of any changes to milestones/deadlines
 - c) The identification of a remediation activity owner /POC
 - d) The justification of estimated resources utilized
 - e) Scheduled completion dates
 - f) The justification of estimated timelines
 - g) Deliverables associated with the defined deadlines (along with acceptance criteria for major deliverables)
 - h) Estimated funding resources required to resolve the identified weakness
 - i) The anticipated source of funding
 - j) Required updates to the POAM based on changes to the control environment
 - h) The quarterly review of the POAM (and status of remediation activities) by the Certifying Official.

2) Update the POAM SharePoint structure to include fields for the relevant missing items above (Scheduled completion date; vulnerability identification source; milestone change and related justification; estimated resources utilized and related justification; justification for scheduling estimates; estimated cost and related justification and funding source).

3) Develop procedures to ensure the enforcement of the policy requirements. For example, develop, follow and document a methodology to justify the resource, budget and scheduling estimates indicated on the POAM.

FY 10 Contingency Planning review

A full BCP (Business Continuity Plan) has not been developed or tested even though FISMA requires the development and annual testing of these plans, so no assurance can be given for its readiness for implementation. Although a Disaster Recovery (DR) Plan was developed on April 14, 2008, it was never rigorously tested (though a table top test was performed), updated or approved. Moreover, 'After Action Plans' were not documented after the initial DR Plan table top test in 2008, therefore, it was not possible for the OIG to assess whether or not issues identified during this process were adequately addressed. This DR Plan outlined the roles and responsibilities for the resources involved in the recovery effort including a line of succession, as well as, restoration procedures for the CPSC infrastructure. However, this Disaster Recovery Plan is not a full Business Continuity Plan and is not fully consistent with NIST SP-800-34 as it addresses only IT processes and does not address non-IT processes. Therefore, this plan does not document a strategy for restoring individual business components such as Laboratory activities as its focus is exclusively on IT functions. Additionally, individual component contingency plans have not been developed to address recovery of individual CPSC GSS components (ex. the major applications) with the exception of one, the CMSRMS (the public facing database).

Furthermore, though the DR Plan was distributed to the appropriate IT resources within the CPSC, it does not address training of CPSC resources on their BCP / DR responsibilities nor does it address DR Plan testing/update/review procedures (timing, frequency and scope). Moreover, this plan has not been updated to reflect the current state of the CPSC IT infrastructure. Additionally, although all critical data is 'Snap-Mirrored' to the file servers in the off-site data storage facility and incremental data backups are performed daily and full backups are performed weekly, these backups are not periodically restored to ensure the data has not become corrupted.

Also, the CPSC does not have an approved Business Continuity policy; however, an unapproved draft policy was developed on May 25, 2010. This draft policy, however, does not define the timing, frequency and scope of the testing of the BCP and DR Plan. Additionally, although the agency performed an overall Business Impact Assessment and included this in the DR Plan in 2008 in addition to having the BIA updated on September 19, 2010 by CRI (an IT consultant), the DR Plan and by extension the BIA was never approved.

FY 10 Contingency Planning Recommendations:

- 1) Develop and implement a DR/BCP Policy with input from each of the CPSC departments to ensure proper policy coverage which is consistent with the NIST SP 800-34 guidance.
- 2) Develop a full BCP (with input from each of the CPSC departments) which is consistent with the NIST SP 800-34 guidance and addresses plan testing, update, QA and review procedures. This plan should include a strategy for the recovery of all business processes not only IT processes.
- 3) Train all appropriate (both IT and Non-IT) resources on their BCP/DR responsibilities.
- 4) The BCP/DR plan (and associated BIA) should be updated and actively maintained to ensure all relevant changes to the business processes and IT infrastructure are reflected in the plan.
- 5) TT&Es (Training, Testing and Exercises) for each of the contingency plans based on requirements outlined in FCD1, NIST SP 800-34 and NIST SP 800-53 should be developed and implemented.
- 6) The CPSC Certifying Official should approve the BCP/DR Plans (and associated BIA) on an annual basis.
- 7) Contingency plans should be developed for each individual system and these plans should be updated annually. Additionally, TT&Es (Training, Testing and Exercises) based on requirements outlined in FCD1, NIST SP 800-34 and NIST SP 800-53 should be developed and implemented for each individual system.
- 8) Annual contingency training, testing and exercises should be coordinated with each of the CPSC branches and be provided to all appropriate resources on their BCP/DR responsibilities. This requirement should be also be defined in the SSP.
- 9) 'After-action' plans should be documented to define remediation tasks developed to mitigate issues identified as a result of the annual BCP tests. The tasks associated with these plans should be documented in the POAM.
- 10) The frequency of the BCP/DR plan reviews, updates and approvals should be documented in the SSP.
- 11) Backup restorations (based on a CPSC defined schedule, but done at least once per year) should be performed to ensure no loss of data integrity.

FY 10 Continuous Monitoring review

Although an assessments of selected security controls (identified as system-specific, hybrid, and common) was performed this year and was documented based on System Security Plan, a Continuous Monitoring strategy has not been approved and documented policies and procedures

for continuous monitoring do not currently exist (though the subject is broached in the C&A policy, approved on September 8, 2010). However, a draft policy (drafted on June 2, 2008) does exist which includes procedures governing the following areas: Configuration Management, Security Control Monitoring and Status Reporting/Documentation. The draft policy, however, does not cover vulnerability scanning, log monitoring, or the notification of unauthorized devices/sensitive new accounts. Therefore, an outside vendor (SecureIT) has been engaged to develop a Continuous Monitoring Plan, in addition to, procedures and a pursuant policy to facilitate the continuous monitoring process. The project to implement this initiative is expected to begin on January 1, 2011, though no completion date has been defined as of yet.

FY 10 Continuous Monitoring Recommendations:

- 1) Develop and implement an OMB/NIST compliant Continuous Monitoring Policy and attendant procedures. These should include requirements to actively monitor logs, detect unauthorized elevation of privileges, identify unauthorized devices on the network and consistently monitor the security architecture for vulnerabilities.
- 2) The SecureIT proposed Continuous Monitoring Plan and strategy should be developed to implement an agency-wide continuous monitoring process. This strategy should include implementing the following processes:
 - a) A Configuration Management processes for organizational information systems (though a configuration management policy exists it has not been fully implemented) *(This recommendation also appears in the Configuration Management section of the report.)*
 - b) Security Impact Analyses on proposed or actual changes to organizational information systems and environments of operation *(This recommendation also appears in the Configuration Management section of the report.)*
 - c) Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy
 - d) Security status reporting to appropriate organizational officials and
 - e) Active involvement by authorizing officials in the ongoing management of information system-related security risks.
- 3) Provide periodic updates to the CIO on the results of the continuous monitoring assessments including additions and changes to the POAM, as well as, the status of the remediation activities and changes to the SSP and SAR.

FY 10 Certification and Accreditation review

As previously mentioned, the C&A process was not formalized through an approved policy and attendant set of procedures until September 8, 2010. Additionally, the policy does not define objective, measurable criteria which can be used to determine if an in-scope system can be certified and accredited, recertified and reaccredited or conversely, decertified. Furthermore, although the C&A policy addresses a process to continuously track changes to information systems that may necessitate reassessment of control effectiveness as defined by SP 800-37, no process is currently in place to continuously track and document the results of these changes.

Additionally, the CPSC contracted with SecureIT (an IT consultancy) to perform their ST&E this year and provide them with the associated SAR. The SAR documents that the CPSC has applied and tested without exception only 114 (43%) of the 261 applicable controls (from a total of 269 defined controls) as defined by FIPS 200 and NIST SP 800-53 (Rev.3) and have not fully satisfied the requirements for the other 147 (35 High, 103 Medium and 9 Low risk) controls (56%). These results show that the minimum baseline security controls have not been adequately applied and as previously mentioned; the Accreditation Official was not presented with the results of this analysis and did not sign off on the receipt of the SAR, the SSP or the POAM until this process was formalized on November 9, 2010.

FY 10 Certification and Accreditation Recommendations:

- 1). Update the C&A policy to include specific, objective and measurable criteria for the certification and accreditation of all in-scope systems.
- 2). Implement the SecureIT recommendations and become compliant with the FIPS 200 and NIST SP 800-53 control requirements.
- 3). Develop and implement a procedure which would track and document the impact of changes to the C&A for all effected systems and ensure the following criteria are included in the change documentation:
 - a). Justification for the ISSO signoff of all change requests with an impact on the GSS LAN. (Ex. the performance of an SIA)
 - b). Evidence of the risk assessment performed by the ISSO to determine the proper course of action regarding what (if any) changes would be necessary to the controls in place as a result of the change.
 - c). The rational / justification for why a change to the SSP (System Security Plan) was or was not necessary.
- 4). The CIO should formally review and signoff on the Risk Assessment, SAR and SSP annually, as well as, sign off on the POAM quarterly.

FY 10 Contractor Oversight review

The CPSC does not have documented policies and procedures regarding the information security oversight of systems operated on the Agency's behalf by contractors or other entities. A procurement Directive (Directive 1522.1) does exist defining what must be included in the statement of work (SOW) associated with contracts of this type (Directive 1522.1: Section 10.D.3); for example, a description of the required deliverables (including reports, if applicable) and a listing of all objectives. Moreover, Directive 1522.1 defines reporting requirements for the third party (Directive 1522.1: Section 10.D.4), Period of Performance (Directive 1522.1: Section 10.D.5), Delivery/Performance criteria (Directive 1522.1: Section 10.D.6) and the Inspection and Acceptance Period which mandates that a deliverable schedule be defined after the contract is awarded. Additionally, the Directive requires that the CPSC define the acceptance criteria for the deliverables (Directive 1522.1: Section 10.D.7). Furthermore, in Appendix G of Directive

1522.1 Project Officers must define realistic delivery schedules and define cost estimates based on the Independent Government Cost Estimates. Even more, Appendix G also requires all contract changes and all contract deadline extensions be approved by the Contracting Officer based on a formal recommendation by the Project Officer. However, Directive 1522.1 does not explicitly address oversight of existing IT systems and services as the individual departments (in conjunction with EXIT) are responsible for this oversight. The CPSC does not outsource its systems to parties outside of the Federal Government and all of the inter-governmental IT relationships are governed through MOU (Memo of Understanding), ISAs (Interconnect Security Agreements) and SOWs. Once procured, the MOUs, ISAs and SOWs are managed, controlled and monitored by the individual departments which are being provided services (in conjunction with EXIT) and no policy is in place to provide guidance/governance over the IT service/system once it is handed over to the individual departments. Moreover, no supplemental policies have been developed to ensure that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines. Furthermore, how scope, budget and schedule changes are monitored and variances reported for a new contracted implementation (ex. Budget variance reporting requirements, requirements traceability matrices, schedule variance reporting etc.) is not defined in the directive and no supplemental policies exist to provide guidance on this process.

Additionally, although a third party systems and services inventory was developed for the FISMA review by EXIT, system generated evidence could not be provided to ensure the completeness of the inventory. Moreover, an inventory of third party systems and services is not maintained and reviewed by the CPSC management to ensure accuracy/completeness. Even more, the inventory does not define the interfaces between the CPSC network and the third party systems. Furthermore, although the MOUs for each of the interfacing entities include IT Security requirements, no process is in place to assign accountability to contractors in the POAM for security weaknesses related to contractor owned systems.

FY 10 Contractor Oversight Recommendations:

- 1) Develop a Contractor Oversight policy to address the governance of third party IT Systems and Services. This policy should outline the roles and responsibilities for the procurement department, EXIT and the individual department utilizing the IT System or Service. Additionally, the policy should address how contract KPIs (Key Performance Indicators) are to be developed, monitored and reported should be developed.
- 2) Procedures for how contract KPIs should be developed, monitored and reported should be defined. These procedures should also be developed for in-house contractors (ex. Helpdesk).
- 3) A third party IT System and Services inventory (which includes all network interfaces) should be developed and maintained by EXIT. Additionally, this inventory should be formally reviewed on an annual basis by EXIT management to ensure the inventory is accurate, complete and current.
- 4) A process should be implemented to assign accountability on the POAM to contractors for security weaknesses related to third party systems/services provided.

2. Security Operational Controls

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

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

Action Taken: CPSC contracted with Patriot to develop the Information System Security Plan (SSP). Patriot reported that in order for 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 SSP.

Due to staffing constraints, CPSC recruited one of the three recommended positions (Information Security Officer) and contracted out the remaining responsibilities on an "as needed" basis. A contract was awarded to PEC Solutions Inc. (PEC) to produce a new SSP that conforms with the resource constraints in place at the CPSC and sets out the specific steps (in the form of recommendations) necessary to implement the plan. The SSP was completed just before the end of FY 03. Implementation of the recommendations contained in the SSP, augmented by new requirement created by subsequent regulations, continued for the next several years. After several years of steady progress a lack of security operational controls played a role in the CPSC's loss of system certification in FY 07. In FY 08, certification and accreditation was regained when the needed security operational control was implemented.

The FY 09 FISMA review found that operational controls in the area of documentation remained problematic. In a number of areas the agency is meeting Federal guidelines in terms of the work being performed, but failing to adequately document what it is doing. For example, although much work has been done to attain and maintain system certification and accreditation at the CPSC, the agency has not documented its policy for establishing a certification and accreditation process that follows the NIST framework (as it is required to do).

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,") However, despite the fact that the FISMA Act (at section 3544(b)(2)(D)(iii)) required each agency to develop

minimally acceptable system configuration requirements and ensure compliance with them, there was no formal agency wide system configuration policy at the CPSC until September 8, 2010. There is also no formal agency policy implementing the procurement policies regarding desktop core configuration, required by FAR 2007-004. These procurement policies were designed to ensure that newly acquired IT equipment complies with the above referenced configuration requirements.

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.

FY 10 Security Configuration Management review

As a result of the OIG's follow up on actions taken to remediate prior findings and the testing for the FY 10 FISMA review several new findings were noted. The CPSC did contract SecureIT to develop a Risk Assessment, SSP, Continuous Monitoring Process, and perform the ST&E in FY 10, however, no defined configuration standards for clients or servers was included in the SSP. FDCC requirements were not mandated by CPSC policy until September 8, 2010 and standard security configurations do not currently exist on either the client or enterprise side of the house. Moreover, the policy does not include language to ensure system configuration requirements are included in relevant IT acquisitions.

Additionally, Configuration Management policies and procedures were not formalized and approved until September 8, 2010 and the associated procedures have not, as of yet, been implemented. Although a standard image is installed on each client machine, security configurations on the client side have not been baselined to ensure compliance with the FDCC requirements. An assessment of NIST FDCC compliance, performed by SecureIT in August of 2010 on a sample population of five client devices, revealed the CPSC was not in compliance with 728 (~50%) of the 1447 configurations included in the NIST FDCC baseline. Additionally, though there are SOPs for building two of the server types used by the CPSC (VM Machines and Windows 2003 Servers), defined security configuration standards do not exist on the Enterprise side. A security configuration compliance assessment, performed by SecureIT in August of 2010 on a sample population of 14 Windows servers (A scan was not performed on the Linux machines due to the inadequacy of the current CPSC tool set), revealed the CPSC was not in compliance with 2335 (~52%) of the 4471 benchmarks defined by the NIST Checklist.gov. Moreover, a list of security configurations does not exist at the Software / Hardware component level (ex. Windows OS, IE, etc...).

Configuration changes follow the informal IT Change Control process [(though the U.S CPSC IT Change Control Policy is referred to in the new Configuration Policy (approved as of September 8, 2010), no such policy exists] and are not tracked separately from other changes. Currently, the Change Control Forms, which are required to be completed prior to a change being implemented, do not provide enough information to make a fully informed determination of how security will be affected as a result of the change. The individuals who are making the

changes are not security experts and since they are not experts, they are not qualified to complete the security impact section of the change control form.

The patch management process is not fully developed and the formal policy and procedures in place governing the Patch Management Process (dated April 1, 2005) are inadequate. They not only require updating and but they have not historically been enforced. All workstations are patched the second Tuesday of each month on "Patch Tuesday" (which aligns with the releases of Microsoft's security patches). Though there is no true development environment for the workstations, when the agency implements a patch/change they use five or so 'test' workstations which are not connected to the network. This is what is used as a development environment and EXIT is able to perform unit and UAT testing, though this is insufficient for integration testing purposes. Once the patch is tested on the test machines they drop the change in production. If any issues arise from the patch/change they remediate at that time. On the Enterprise side, the agency does not have a process in place to systematically identify flaws and implement patches; instead all servers are patched manually. This has lead to several machines missing the latest patches (some have not been patched since 2006). Additionally, the 88 Windows servers have a total of 3732 applicable updates which are not currently installed (this number includes critical and security patches).

A software inventory was developed for the annual SAR review, however, though the Software Inventory was developed to be consistent with the boundary of the information system and is available for review/audit by designated organizational officials, the level of granularity deemed necessary for tracking and reporting is inadequate. The Software Inventory report does not provide sufficient granularity to achieve necessary property accountability; license compliance is impossible to assess with this level of reporting. Additionally, there is no software license tracking and reporting process in place. Meaning, the CPSC does not employ a tool or process which identifies the number of software instances on the network to ensure it is in compliance with the number of software licenses possessed. Furthermore, a software inventory scan is run on an annual basis and the current guidance is for the scan to be run monthly. Even more, a random audit in FY 09 revealed several instances of unauthorized software on client machines and though EXIT is working on a process to address this issue, it has not been remediated as of yet. While the number of users with local administrative privileges to their machines has been limited to 10 (three EXIT users, 4 IT Contractors, two Program Analysts and one Finance user who require this access per their job functions) as of September 27, 2010, prior to July 16, 2010 (the date the initiative to limit this access began) 130 users had local administrator access to a total of 156 machines which severely limited management's ability to track what individual users have downloaded. Additionally, a scan has not been performed to identify all individual instances of software on client machines.

FY 10 Security Configuration Management Recommendations:

- 1) Update the current Configuration Management policy to include the following.
 - a) How to report on Security Configuration Changes separately from other typical changes.
 - b) A specific protocol to require the resource completing the Change Management Form to create a formal Security Impact Analysis (SIA) (which includes sufficient granularity to allow the security resource responsible for the walkthrough and approval of the change to

justify the approval decision) as a way to capture all relevant system security impacts and include it in the change management packet.

- 2). Develop and enforce a process to govern software license compliance:
 - a) Limit the number of local administrators to only those who require the local administrative access to perform core functions of their job.
 - b) Identify the number of software licenses which are installed on each machine.
 - c) Reconcile the list of software instances to the software licenses owned by CPSC and remediate any discrepancies. Add the number of software instances residing on each machine inventoried to the Software Inventory report.
 - d) Implement a process which requires all future installations of software requiring a license (ex. Microsoft, Oracle, etc.) to be added to the Software Inventory report.
- 3) Create a security baseline which is in compliance with the Federal guidance for all H/W and S/W components.
- 4) Once a Security Baseline Configuration is developed and implemented, implement a solution to continuously scan the network for any deviations to the standard security configurations. The results and analysis of this scan should be included in the monthly Continuous Monitoring Reports.
- 5) Build a development environment and test all patches in the development environment prior to rolling them into production.
- 6). Once the development environment is in place and Security Configuration gaps are identified, the gaps should be documented, prioritized and remediated.
- 7) Once the gaps are remediated and the CPSC is in compliance with the FDCC requirements, a change management process to govern all changes to this baseline (ex. through the use of a configuration library) should be developed.
- 8) Patch all servers which are not up to date or provide a formal justification for not implementing the patch.
- 9) Implement a process (and formalize this process by updating and enforcing the patch management policy) to systematically update all server's security patches based on Federal Guidance and industry best practices where federal guidance is not available.
- 10) Implement a tool to scan the network for non-compliance with current patches and report the results of these scans in the monthly Continuous Monitoring Reports.

FY 10 Security Incident Management review

Though an approved Security Incident Management Policy does exist, this policy has not been updated since 2005 and has not been disseminated to the NEB/CUSB teams. Moreover, the policy does not document a required reporting process which outlines all of the individual user

and department responsibilities. Furthermore, the formal procedures are documented by the ISSO in the IT Security Incident Reporting SharePoint tool; however, these procedures have not been disseminated to the appropriate resources (ex. NEB/CUSB). Also, the policy in place states: "US-CERT defines an incident as an event violating an explicit or implied security policy. These incidents include, but are not necessarily limited to, attempts (either failed or successful) to gain unauthorized access to a system or data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent" however, there is no monitoring/documenting/reporting of the following types of events by the resources (NEB/CUSB) who's responsibility it should be to monitor and report these events: attempts (either failed or successful) to gain unauthorized access to a system or data; unwanted disruption or denial of service; and the unauthorized use of a system for the processing or storage of data.

As the NEB and CUSB teams do not document security incidents, a comprehensive analysis, validation and documentation of incidents cannot be performed. Additionally, though the following tools are in place to monitor for Security Events: ISS RealSecure (IDS), Blue Coat (internet filter), Barracuda (spam firewall/malware scanner), Kaspersky (endpoint security), Forefront (email security/malware scanner), CheckPoint firewall and eEye Retina (vulnerability scanner), these tools only monitor for outside threats. Currently, nothing is in place to monitor for internal threats such as elevation of privilege attempts to obtain unauthorized administrator rights. Although VPN and Firewall logs are kept and alerts are sent in the event of pre-defined security events, these logs are not analyzed and reported in any meaningful way. This is due to the lack of a log monitoring and reporting tool. Currently, logs have to be pulled manually from each individual server which is a manually intensive process, making it impractical to perform and report on such analysis.

Though there is an OMB directive in place requiring the ISSO to contact US-CERT within a defined timeframe based on the classification/type of security event (ex. one hour for potential exposure of PII); this process is not always effective. Security incidents were not tracked prior to August 13, 2010 and US-CERT was not notified within the established timeframe of one hour for the only documented case of a reportable security incident response available for audit review.

FY 10 Security Incident Management Recommendations:

- 1) The Security Incident Reporting Policy should be updated to include the roles and responsibilities for all resources involved in the monitoring and/or reporting of Security Events especially, those who are directly involved in the monitoring, documenting and/or reporting of such events.
- 2) The Security Incident Reporting policy and procedure documents should be disseminated to all appropriate parties.

3) Users responsible for the monitoring and reporting of Security Incidents should be trained on the procedures the ISSO has implemented and the use of the new tool the ISSO has implemented to track and report on Security events.

4) All security incidents should be tracked in the SharePoint tool going forward. VPN and Firewall alerts (based on a NEB defined set of criteria) should be filtered through the HEAT ticketing system to the ISSO SharePoint so all incidents are tracked and remediation documented. Additionally, the CUSB team should log all incidents with security ramifications through HEAT and into the SharePoint solution.

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

6). Implement a product that automatically detects malicious network activity, and creates alerts when one of the predefined signatures is triggered (such as Einstein 2 or an equivalent product). This type of product will also alert US-CERT directly when specific malicious network activity matching the predetermined signatures is detected allowing the CPSC to utilize US-CERT expertise.

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

Security Awareness Training:

Documented policies and procedures for security awareness training exist; however, they are outdated (last updated in 2006) and do not reflect the current process. For example, the policy requires the ISSO to send an email informing all new CPSC employees and contractors to complete the Rules of Behavior form on CPSC net within the first 5 business days of their assignment. This is now required as part of the on-boarding process and is signed as part of the new hire paperwork.

Due to the migration to a new product to provide Security Awareness Training and the inadequacy of the new product's reporting capability, an accurate and complete inventory of who had received the mandatory Security Awareness Training could not be developed by CPSC management. Therefore, since training completion statistics provided by management could not be relied on, the OIG cannot attest that at least 90% of the required CPSC users received the Security Awareness Training. Additionally, as of November 10, 2010, the best estimate available (unsubstantiated by reliable reporting) indicated that only ≈68% of total CPSC staff and contractors with access to the CPSC system had completed security awareness training which is well below the 90% FISMA requirement.

Moreover, the OIG cannot attest to the adequacy of the content of the specialized training for users with elevated privileges because the training course was not selected in time for the OIG to review the course materials prior to the end of the fieldwork. However, as of November 10, 2010, when the final security training numbers were reported only $\approx 73\%$ of the CPSC network users with elevated privileges had completed this specialized training well below the 90% FISMA requirement. Furthermore, a recommendation from the FY 09 FISMA review recommending that training on the CPSC's policy regarding peer-to-peer file sharing be added to the Security Awareness Training curriculum has not, as of yet, been implemented.

FY 10 Security Awareness Training Recommendations:

- 1) Update the Security Awareness Training policies and procedures to reflect the current processes (ex. Rules of Behavior are now required to be signed as part of the on-boarding process.)
- 2) CPSC management should select a NIST SP 800-50/SP 800-53 compliant training course for all users with elevated privileges and provide this training to all appropriate resources.
- 3) Implement a Security Training Solution with reporting capabilities sufficient to adequately document who has successfully completed and who has not successfully completed the Security Awareness Training course OR enhance the current solution's reporting capabilities to ensure adequate reporting is possible.
- 4) Add training on the CPSC peer-to-peer policy to the Security Awareness Training curriculum.

3. Security Technical Controls

Prior Finding: Security technical controls are specific to the system's ability to identify, track, and act on authorized or unauthorized usage. Because CPSC management had not implemented sufficient technical controls in the areas of identification and authentication, logical access, and audit trails, CPSC management had left sensitive information vulnerable. This condition appears to have been due to CPSC management not having the resources necessary to make implementation of sufficient technical controls a priority. The level of risk was rated high for identification and authentication, and logical access.

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

Action Taken: The effectiveness of six of CPSC's systems and the underlying elements of each were tested during the FY 2001 audit. Weaknesses identified in controls related to these systems contributed to the overall condition of CPSC's information security program. Management was advised of specific weaknesses and recommendations, each of which was to be addressed during the implementation of the SSP and Systems Certification and Accreditation contract. Weaknesses outlined in the SSP were to be corrected in all applications. Additional

systems were not tested because management was in the process of implementing prior recommendations, the implementation of which would alter the policies and procedures applicable to all applications. As reported in the management response to the original audit, CPSC requested funding in Fiscal years 1999 through 2002 without success to establish a capital budget for information technology. The need for such funds was also included, unsuccessfully, in CPSC's FY 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, CPSC has applied some savings from operating funds to this area. In FY 02, 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 EXIT commitment was \$714,891 in the form of salaries and other expenses. In FY 04, 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 10, the CPSC's commitment rose again to \$18,884,618 [\$9,371,016 for EXIT-IT (which included the creation of a 'sub-budget' for Capital Replacement of \$1,000,000) and \$9,513,602 for EXIT-AS respectively] and 34 FTEs. Work on implementing the recommendations contained in the SSP and more recent guidance continues.

In some cases the implementation of security controls has outstripped the documentation or generation of policies regarding same. In other cases, where the agency has developed policies, it has failed to provide agency wide training detailing them to its workforce. For example, the CPSC conducts continuous intrusion detection monitoring and remediates the issues identified, but these efforts are not formally documented or covered by existing policies.

On the other hand, the agency has a policy prohibiting its employees from using peer-to-peer file sharing on Government computers, but does not explain this policy in its information security awareness, ethics, or any other agency wide training.

In FY 09, the CPSC's Plan of Action and Milestones (POAM) report to OMB reflected the improvements that the CPSC has made as well as the work remaining before it. The agency had then resolved all material weaknesses, as well as, the "high" security vulnerabilities found by Grant Thornton and the 2007 STE Evaluation. However, it had failed to address all of the lower priority vulnerabilities found by these evaluations or to keep up with some of the FY 09 security requirements. The CPSC had failed to adequately address approximately thirty-nine (39) identified weaknesses, one of which was rated as a "high" security vulnerability and sixteen (16) of which were rated as medium security vulnerabilities

The CPSC acknowledges its need for continued improvement. Over the past few years, the CPSC has met the following goals in its effort to improve its security technical controls: implementing a security awareness training program, providing a redundant cooling capability to the Agency's existing computer room air conditioning unit, providing the ability to quickly recover from an e-mail server failure by periodically taking and storing e-mail "snapshots" of the

e-mail database, implementing the ability to perform automated system auditing, and implementing the monitoring of Internet usage.

Although they are properly reflected in the POAM, a total of 22 (17 Moderate and 5 Low) weaknesses have not been remedied. Perhaps more troubling, no firm plan for how to address them or scheduled completion dates have been established for them. For example, one of the moderate issues has been open since 2009 and has been signified in the POAM as 'Researching' with no follow-up actions documented. Moreover, the actions taken to close issues signified as 'Closed' or 'Resolved' have not been documented. Furthermore, client sessions are not automatically terminated after the NIST specified 30 minute period of inactivity; the POAM shows the issue as 'Closed' and the CPSC did not document their justification for this signification.

FY 10 Remote Access Governance Review

Currently, there are no formal documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access. There are, however, rules of behavior (which must be signed by all new CPSC employees prior to users being granted access to the CPSC network) which establish General Use, Security (to a limited extent), Software/Hardware installation, email use, PII and Social Networking rules. Additionally, a Teleworking policy exists outlining limited terms and conditions for Teleworkers and a proposed (though unapproved) General Access Policy was drafted on April 10, 2010 that documents some of the requirements outlined in the NIST 800-53 guidance. For example, the policies document allowed methods of remote access to the information system, establishes usage restrictions and implementation guidance for each allowed remote access method and monitors for unauthorized remote access to the information system. These policies do not, however, explicitly cover all of the required items in NIST 800-53, for example, 'the technical characteristics of the telework or remote access solution and related components'. These characteristics include the authentication methods; the cryptographic mechanisms used to protect communications; and firewalls and other mechanisms used to control access to networks and resources on those networks'. NIST required 'technical characteristics' also include, 'Ensuring that each remote access infrastructure component (servers, gateways, authentication servers, etc.) has its clock synched to a common time source so that its timestamps will match those generated by other systems'; 'Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.'; and, 'Detecting and documenting anomalies detected 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 and the agency should carry out, 'The periodic performance of assessments to confirm that the organization's remote access policies, processes, and procedures are being followed properly'.

Additionally, requirements in the draft policy are not yet fully enforced. For example, though the draft policy does address the NIST 800-53 (AC-17) requirement, 'Authorizes remote access to the information system prior to connection & enforces requirements for remote connections to the information system,' by requiring all users connecting remotely to utilize level three e-

authentication (multi-factor authentication) prior to establishing the connection; level 3 multi-factor authentication is not programmatically enforced as of yet.

The CPSC utilizes several techniques to protect against unauthorized connections and subversion of authorized connections, however, an e-authentication analysis has not yet been performed (and the results implemented) to ensure proper compliance with the NIST standards. Additionally, though VPN traffic is logged and firewalls are configured to alert security engineers of a predefined set of security events, VPN and firewall logs are not actively monitored. CPSC management has attributed this to current system limitations making the active monitoring of these logs impractical and to an overall lack of resources. Additionally, users accessing the network are not uniquely identified and authenticated. Although all of the field and corporate users outside of EXIT are uniquely identified and authenticated, six NEB users (domain administrators) utilize the Windows Administrator account rather than being provided individual, local, admin accounts on the machines for which they are responsible.

The CPSC requires all data to be transferred across the VPN to be encrypted. This is programmatically enforced through the use of Digital Certificates which are added to all new machines upon imaging and assignment. However, data stored on mobile devices and removable media such as CDs and flash drives are not encrypted. Additionally, all Laptops are supposed to have their hard drives encrypted through the use of Guardian Edge. Compliance with the hard drive encryption requirement can be verified through the Guardian Edge console for all except for approximately 100 client machines (NEISS machines which have stand alone instances of Guardian Edge). As a result of the OIG review of the Guardian Edge console, however, it was noted that of the 23 client machines sampled one machine (~4%) had not been encrypted through the tool. Moreover, although an SOP exists illustrating how the NEISS machines are to be set up, the SOP did not include a section which required Guardian Edge to be installed until this finding was shared with CPSC management on September 23, 2010; therefore, documentation of the encryption of the NEISS machines could not be provided.

FY 10 Remote Access Governance Recommendations:

- 1) Develop and implement a single policy which addresses all aspects of Remote Access, including the monitoring and logging of such access, in addition to the following topics:
 - a) The technical characteristics of the telework or remote access solution and related components. These include the authentication methods; the cryptographic mechanisms used to protect communications; and firewalls and other mechanisms used to control access to networks and resources on those networks.
 - b) Ensuring that each remote access infrastructure component (servers, gateways, authentication servers, etc.) has its clock synched to a common time source so that its timestamps will match those generated by other systems.
 - c) Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
 - d) Detecting and documenting anomalies detected 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.

- e) EXIT periodically performing assessments to confirm that the organization's remote access policies, processes, and procedures are being followed properly.
- 2) Actively monitor remote user logs. This may be facilitated by the implementation of the Novell Sentinel (or equivalent) tool. Additionally, results of these analyses should be reported to the ISSO (and all other appropriate parties)
- 3) Perform an E-Authentication analysis on all in-scope systems or require multi-factor authentication in order to access the CPSC network.
- 4) Develop and implement Baseline Security Configurations on both the clients and servers. Additionally, implement a continuous monitoring program to identify any variances to the active client/server security configurations. *(This recommendation also appears in the Configuration Management section of the report)*
- 5) All security incidents should be tracked in SharePoint going forward. VPN and Firewall alerts (based on a NEB defined set of criteria) should be filtered through the HEAT ticketing system to the ISSO SharePoint so all incidents are tracked and remediation documented. Additionally, the CUSB team should log all incidents with security ramifications through HEAT and into the SharePoint solution. *(This recommendation also appears in the Security Incident Management section of the report)*
- 6) Implement a solution which encrypts all removable media (ex. UBS devices, CD/DVD drives, etc.) which have been connected to the CPSC network.
- 7) Include a protocol requiring a standalone instance of Guardian Edge to be installed on all NEISS Machines prior to their roll out in the NIESS Machine Setup SOP. Additionally, track all such installations through HEAT for documentation purposes. Moreover, consolidate the separate Guardian Edge databases into a single instance, remove old machines no longer connected to the network and develop effective, consolidated reporting from the tool.
- 8) Encrypt all machines or obtain waivers documenting why these machines are not encrypted.
- 9) Domain Administrators should be granted individual, local, administrative accounts on the machines for which they are responsible. Only one person should know the Windows Administrator password and the password should be checked in/checked out when this access is required.
- 10) Configure remote sessions to time out after 30 minutes.

FY 10 Identity Management review

No approved policies and procedures exist for account and identity management. Draft policies and procedures were documented as of April 12, 2010; however, these policies were not approved and have not disseminated throughout the agency. Additionally, although the draft CPSC policy addresses purpose, scope, and compliance, it does not address or contain roles and

responsibilities, management commitment, or coordination among CPSC branches. Moreover, the procedures do not address achieving this policy. For example, the policy and procedures state that there will be an account lockout after a number of unsuccessful login attempts; however, the number of actual unsuccessful login attempts is never defined.

CPSC manages all aspects of CPSC information system accounts which include authorizing, establishing, activating, modifying, reviewing, disabling and removing network accounts. All users (including contractors) with access to the CPSC network are provided with an email address and defined within AD prior to be able to access to the network. Additionally, all user accounts which authenticate through e-directory (which accounts for the vast majority of user accounts) are informally reviewed by the ISSO (using BindView, a third party application) on a monthly basis for appropriateness, though this review is not documented. However, BindView does not include non-user accounts and it does not include AD accounts. AD accounts (both user and non-user accounts) are not inventoried and a complete inventory of these accounts cannot be produced with the current CPSC toolset. Moreover, all CPSC users have remote access to the CPSC network on their laptops, however an E-Authentication Analysis has not been performed and Multi-factor authentication is not currently required for all users.

Only EXIT staff members are Domain Administrators, specifically, the six NEB members and seven members of the CUSB who require this access to perform their day to day duties, however, there is no logical segregation between the security administration and audit logs maintenance. Additionally, if a non-Domain Administrator requires access to the network this access is requested via the formal process (e.g. submission of a Heat ticket), however, if a user requires Domain Administrator access this request is provided informally and does not follow the standard process (it is not tracked in Heat). Moreover, the CPSC has not implemented the principle of least privilege as the level of granularity in the documentation related to the assignment of user accounts is not sufficient to enforce least privilege. This has caused user privileges to not be consistent with documented user authorizations. Some users have been given greater access than their documented authorizations allowed.

All non-client machines attached to the network use a static IPs (falling within a specified IP range) for identification and all client machines (sans the network administrators machines who also use a static IP) utilize a dynamic IP (falling within a defined DHCP range) to identify them. This is how CPSC distinguishes devices that are attached to the network from users. However, no Mac Filtering or RADIUS (Remote Authentication Dial In Service) is performed to uniquely identify and authenticate each machine to the network prior to establishing the connection.

Procedures for employee separation are as follows: EXRM submits an "Employee Departure" request via the Employee Departure application in FPPS once they review the SF-52 data for accuracy and completeness. Once this request is generated, a HEAT ticket is automatically generated to notify relevant CPSC staff (including members of the DTS Employee Update list in Active Directory, which includes TSCS and TSHD) of the departing employee. Once CUSB is notified about a termination through HEAT, they revoke access immediately as a matter of practice; however, the OIG noted that this process is not always effective. The OIG discovered three instances where departing Federal Employees had not had their access revoked once terminated. EXRM has attributed this to a system limitation in FPPS which does not allow a

departing federal who had previously separated once to enter their name into the system again if they have to separate a second time from the agency. This situation can be a result from an employee being rehired or reassigned. CPSC employees are frequently rehired (ex. returning summer interns) which was the case in all three of the noted exceptions. The breakdown in this process has led to CUSB not being notified of an employee departure through the HEAT ticketing system. Although, there is a mitigating control in place where EXRM provides CUSB a weekly staffing report to notify them of all pending new hires, departures and promotions the process failed.

For contractors, the departure process is entirely manual as contractors are not entered into FPPS for processing. Instead, a manual form is filled out by the contractor/contracting company related to the departure of the contractor and the form is then provided to EXRM and EXIT. Additionally, unlike Federal Employee Departures, EXIT is not sent a weekly report by EXRM notifying them of departing contractors. The OIG noted that this process is also not always effective. The OIG discovered one instance (10% of a total population of 10 departing contractors) where a departing contractor had not had their access revoked once terminated. EXRM has attributed this breakdown to the process being overly manual and to non-adherence by the contractors. Additionally, a contributing factor has been attributed to the fact that no centralized contractor database housing HR information such as hire and departure dates is employed which EXRM can readily query. EXRM's ability to effectively notify clearing officials of all separating contractors on a periodic basis, which would mitigate some of the risk of this manual process, is adversely impacted by the lack of the above described database.

FY 10 Identity Management Recommendations:

- 1) Develop and document an Identification and Authentication policy with attendant procedures which includes roles and responsibilities, management commitment and coordination among CPSC branches. Then once these policies and procedures are approved, disseminate them to all of the appropriate resources throughout the agency.
- 2) Implement a solution to inventory and report on all AD and E-Directory accounts [both user (login) and system (no login) accounts].
- 3) Formally review the AD and E-Directory logs on a monthly basis and include the results of this review in the Continuous Monitoring Report.
- 4) Implement (and document) the principle of least privilege (documenting waivers to standards where required) to all CPSC network accounts and ensure all user privileges granted are consistent with user privileges authorized.
- 5) Activity logs of all administrative/super user accounts should be monitored.
- 6) Domain Administrator's access to update audit logs should be revoked.
- 7) Require new Domain Administrators to follow the formal user access request process.

- 8) Revoke the access of terminated users.
- 9) Implement a solution to systematically disable users after 30 days of inactivity.
- 10) Improve the revocation procedures by:
 - a) Configure FPPS to allow rehired/returning Federal Employees to systematically request a separation.
 - b) CUSB should formally reconcile the current separations, as indicated on the weekly HR Staffing report, to all CPSC IT system ACLs to ensure all user accounts are adequately revoked.
 - c) A central contractor database which maintains records of all current and separated contractors should be developed and linked to the FPPS application to allow adequate reporting of contractor separations. The proposed WTTS EOD (Workforce Transformation Tracking System – Entry On Duty) solution (an NBC hosted system) will assist the CPSC in ensuring separated contractors are adequately processed and user access is revoked in a timely manner.
- 11) Perform an E-Authentication analysis on all in-scope systems or require multi-factor authentication in order to access the CPSC network. (*This recommendation also appears in the Remote Access Governance section of the report*)
- 12) Define and document a list of devices for which identification and authentication is required before establishing connections to the GSS and implement a tool (ex. IEEE 802.1X or equivalent) which uniquely identifies and authenticates devices prior to establishing a connection to the CPSC GSS.
- 13) Implement a tool (ex. BigFix, Zenworks 11 or equivalent) which inventories all servers, network devices and PC's on a network and reports back with complete information about OS, service packs, hot fixes, hardware, software, firmware, running processes, etc. on local and remote machines.

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

After the STE Evaluation in FY 07 resulted in the decertification of the CPSC's system, much work was put into regaining system certification, which was achieved in FY 08. NIST 800-53 controls were incorporated by the agency and future certification and accreditation work should have been consistent with the most recent NIST Special Publication requirements. It was assumed at this time that the remaining security vulnerabilities would be addressed as expeditiously as possible. However, in FY 09, it was found that only 5 of the existing 63 vulnerabilities shown in the 2007 STE Evaluation had been addressed. Moreover, the results of the ST&E performed in FY 10 reflected a high number of control deficiencies [147 (~56%) of the applicable 261 NIST 800-53 controls] which have to be addressed as soon as possible.

FY 10 Performance Measure Recommendations

- 1) Implement the SecureIT recommendations and become compliant with the NIST SP 800-53 control requirements.

- 2) Once the SecureIT recommendations have been implemented, the NIST SP 800-53 controls which were not fully satisfied at the time of the 2010 ST&E should be retested to ensure the C&A of the GSS LAN will be possible in 2011.