U.S. CONSUMER PRODUCT SAFTEY COMMISSION

OFFICE OF INSPECTOR GENERAL

FY 2015 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW REPORT

Issued: 12/8/2015

This report conveys the results of the OIG's review of the CPSC's compliance with the Federal Information Security Management Act (FISMA).

U.S. CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Christopher W. Dentel
Inspector General

Tel: 301 504-7644
Fax: 301 504-7004
Email: cdentel@cpsc.gov

Date: December 8, 2015

TO : Elliot F. Kaye, Chairman
Robert S. Adler, Commissioner
Marietta S. Robinson, Commissioner
Ann Marie Buerkle, Commissioner
Joseph P. Mohorovic, Commissioner

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Federal Information Security Management Act (FISMA) Evaluation

The Federal Information Security Management Act (FISMA) requires that the U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conduct an independent evaluation of the CPSC's information security program and practices. In evaluating the CPSC's progress in implementing its agency-wide information security program, we specifically assessed the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB).

This year's FISMA evaluation found that although management continues to make progress in implementing the FISMA requirements much work remains to be done.

The OIG noted 49 findings in this year's FISMA review. These findings and the areas identified as requiring improvement are detailed in the attached report.

Should you have any questions, please contact me.

Christopher W. Dentel

Christopher W. Dentel
Inspector General

Table of Contents

EXECUTIVE SUMMARY

The U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conducted an independent evaluation of the CPSC's information security program and practices. This report serves to document the CPSC's compliance with the requirements of the Federal Information Security Management Act (FISMA). In evaluating the CPSC's progress in implementing its agency-wide information security program, we specifically assessed the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB).

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements. The CPSC's accomplishments in implementing FISMA requirements include:

- ✓ The completion of the General Support System (GSS LAN) security accreditation process and maintaining an active security accreditation.
- ✓ The Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDSRAM) application, and the CPSC public website, www.cpsc.gov, completed independent security assessments and retain active security accreditations.
- ✓ The Cyber Security Incident Response Team (CSIRT) continues to improve its processes as it matures by refining Standard Operating Procedures (SOPs), implementing new solutions, and improving existing solutions to facilitate the identification of security incidents.
- ✓ The CPSC has increased staffing resources, to include a Chief Information Security Officer (CISO), to assist with IT security efforts.

The CPSC's continual improvement in system reporting and monitoring capabilities, combined with the CPSC's maturing incident handling process, has positioned the agency to take proactive steps to address known and potential vulnerabilities. However, the OIG identified several security weaknesses in the CPSC's management, operational, and technical controls policies, procedures, and practices. The conditions outlined in this report could result in 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.

The OIG noted 49 findings in this year's FISMA review. The IT challenges currently facing the CPSC are particularly relevant as the agency continues to deal with the implementation of the Consumer Product Safety Improvement Act (CPSIA), specifically with the CPSIA's impacts on the agency's IT operations. We identified the following areas as requiring improvement:

- ✓ Configuration Management
  - – Lack of a comprehensive hardware/software inventory;
  - – Management has not documented and implemented all the security configurations outlined by the United States Government Configuration Baseline (USGCB) and the National Vulnerability Database (NVD) or assessed the risks associated with all of the deviations from these baselines; and

  - Agency systems were not patched in a timely manner.

- ✓ Identity and Access Management
  - The CPSC has not implemented the Principle of Least Privilege and proper segregation of duties for the GSS LAN; and
  - Account modification procedures lack proper documentation/implementation; and adequate controls have not been implemented for shared user accounts.

- ✓ Incident Response
  - Dates and times relevant to events associated with incident resolution have not been adequately documented by management.

- ✓ Risk Management
  - Implementation of the National Institute of Technology and Standards (NIST) Special Publication (SP) 800-37 is incomplete;
  - Information systems outside of the GSS LAN security boundary are not accredited; and
  - An inventory of major systems has not been defined and certified.

- ✓ Security Training
  - CPSC resources with significant security responsibilities have not been provided role-based training.

- ✓ Plan of Actions and Milestones (POAM)
  - Consistent updating of all agency POAMs did not occur in FY 2015 nor did the POAMs include all requisite information.

- ✓ Remote Access Management
  - Lack of implementation of Federal Information Processing Standards (FIPS) 140-2 required encryption for remote access connections and monitoring of remote access connections.

- ✓ Contingency Planning
  - Lack of a Business Impact Assessment, a Business Continuity Plan (BCP), a Disaster Recovery (DR) Plan, and a Continuity of Operations Plan (COOP). Further, the CPSC has not formalized or tested a current Information System Contingency Plan (ISCP).

- ✓ Contractor Systems
  - Interconnection Security Agreements were not established and/or updated for all relevant CPSC third party systems. Further, an assessment of all relevant security controls associated with the systems did not occur.

- ✓ Continuous Monitoring–
  - The OIG assessed the CPSC's continuous monitoring efforts over IT security using the Information System Continuous Monitoring (ISCM) Maturity Model.

The maturity model consist of five levels, our assessment found that the CPSC has only achieved level one, the lowest level, in each of the domains (people, processes and technology).

MANAGEMENT’S RESPONSE

Overall, based on the management’s response, we have concluded management did not concur with all of our findings and recommendations. Management indicated that they did not have adequate time to respond to a number of findings. However, when management was asked how much additional time they would require they failed to respond.

RESULTS AND FINDINGS

Risk Management

FISMA requires security authorizations for all systems operated by the agency. FISMA also requires management to assess and monitor security controls on a continuous basis using a risk-based approach based on, amongst other guidance, FIPS and NIST guidance. Once management performs the initial authorization of a system, management should use the results of on-going security assessments and monitoring tasks, as a basis for each system's continuing Authorization to Operate (ATO). This requires management to develop a process and establish an infrastructure to frame, assess, respond to, and monitor risk.

Progress:
The CPSC has begun to update the control implementation catalogs associated with the agency's authorized systems, to align with the latest revision of the NIST SP 800-53 guidance, released in April of 2013. According to management, they have completed approximately 75% of the updates and estimate completion will occur during FY 2016. In addition, management updated the System Security Plans (SSPs) for the agency's accredited systems in FY 2015. Furthermore, management began to issue, on a sporadic basis, security status reports to Senior IT management to provide them with updates on the known elements of the agency's security posture.

To Be Addressed:	**Management Response:**
The CPSC does not manage risk from an organizational perspective. For example, Management has not: • Created an Organization-wide Risk Management Strategy to ensure risks to the mission and organization are considered. Developed and implemented an adequate process to define and accept risk when authorizing a system to operate. • Defined the methodology used to calculate the agency's Organizational Risk Tolerance or implemented a process to determine if existing risks are within the organizational risk tolerance. • Defined objective and measurable criteria used to justify the accreditation and reaccreditation, or conversely, decertification of in-scope systems. • Established a Risk Executive (function) or established a comprehensive governance structure to manage risk.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond to this finding. However, when management was asked how much additional time they would require they failed to respond.*

• Developed an EA, and, therefore, management has not integrated the EA into the agency's risk management process.	
The CPSC has not developed an inventory of major applications and provided the inventory to the Agency Head for certification, as required by FISMA, section 3505(c)(2). As a result, not all CPSC systems have been inventoried, categorized, or authorized. Additionally, management has not selected, implemented, or assessed all security controls required to be employed/authorized by all agency systems.	*Concur.*
Management did not update security documents throughout the year to provide an up-to-date view of the information systems' security posture and provide a method of continuously monitoring those postures, as required by NIST SP 800-37. While, the IT Security Team does maintain POAMs for agency systems, management did not update the POAMs throughout the year nor consistently brief Senior Management on the POAMs remediation efforts quarterly, as required by NIST guidance.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond to this finding. However, when management was asked how much additional time they would require they failed to respond.*
The CPSC's existing SSPs do not include all required information. We identified that: • The SSPs for the agency's accredited systems do not reflect all the changes in the April 2013 revision of NIST SP 800-53. • Management has not selected all of the NIST SP 800-53 security controls for a moderate impact system or documented the justification for not implementing these controls. • Management has not documented how all of the agency's selected controls were parameterized and implemented for the agency's accredited systems. • A description of the agency's minor applications within the security boundary of the GSS LAN was not provided in the GSS LAN SSP . Management did not include all system components in the description of the GSS LAN security boundary.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond to this finding. However, when management was asked how much additional time they would require they failed to respond.*

The CPSC has not defined what types of threat activities senior officials must be briefed on, how often senior officials must be briefed on threat activity, and which senior officials require this briefing. The IT Security Team sporadically sends out emails regarding current and relevant threats (such as, warnings about phishing schemes and malware affecting the agency and agency resources) to the entire agency and notifies senior IT officials of confirmed security incidents. However, the IT Security Team does not regularly brief senior officials on new, emerging, and advanced persistent threats and threat events.	*EXIT does not concur*.

Recommendations:

1. Management should develop and document a robust risk management process led by the Risk Executive (function). The Risk Executive (function) should report to a governing board that includes senior management.

2. 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. These techniques and methodologies should include objective, measurable criteria that management uses to justify the certification and accreditation, recertification and reaccreditation, or conversely, decertification of an in-scope system;
    b. The types and extent of risk mitigation measures the organization plans to employ to address identified risks;
    c. The level of risk the organization plans to accept (i.e., organizational risk tolerance), and the methodology used to calculate the organizational risk tolerance.
    d. 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
    e. The degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

3. Management should develop a comprehensive Enterprise Architecture (EA) and integrate the EA into the risk management process.

4. Management should actively update and maintain security documentation for all agency systems (ex. SSPs, Security Assessment

Reports, Risk Assessments, and POAMs) each time a weakness is identified/remediated, or a change with a security impact is made. Agency SSPs should be maintained as a "living documents" to facilitate on-going risk management decisions. As updates are made to these documents, they should be provided to the relevant information system owners, common control providers, senior information security officers, and authorizing officials to assist in the ongoing management of information-system-related security risks.

5. Management should create/update security plans for all major agency systems and include all NIST SP 800-53, Revision 4 selected controls in these plans.
6. Management should update existing security plans to describe how the NIST SP 800-53, Revision 4 controls are parameterized and implemented.

7. Management should update the existing security plans, where applicable, to include all minor applications and a description of how the controls selected for each of the minor applications are implemented.

8. Management should include a description of all system components within the GSS LAN security boundary in the GSS LAN SSP.

9. Establish a process that requires the IT Security Team to brief management on threat activity. According to NIST SP 800-30, threat events can be described as: confirmed, expected, anticipated, predicted, possible, or not applicable. This information can be obtained from a combination of sources, such as continuous monitoring solutions indicating a particular threat event and from sources like the Internet Storm Center (SANs) and Common Attack Pattern Enumeration and Classification [CAPEC] (https://capec.mitre.org/) describing current threat events in the public sector.

10. Management should document and certify a systems inventory that includes all CPSC systems (both major and minor systems) and includes a description of each system in the systems inventory.

11. The Agency Head should review and certify the inventory of major systems annually and in the event of a major change. Ultimately, this inventory should tie to the agency’s EA. The major systems inventory should include:
    a. the interfaces with all other systems/networks,
    b. the system criticality (based on a current BIA),
    c. the security categorization (based on FIPS 199),
    d. the hardware utilized by the system,
    e. the databases utilized by the system,
    f. the ATO status of each system, and

g. the name of the system owner.

12. Management should select, implement, and assess the security controls employed by each of the agency systems, including the agency's minor applications. Management should include this information in the existing risk documentation, where appropriate.

13. Management should formally authorize the operation of the all agency systems, including the agency's minor systems, once the risk associated with those systems is known and accepted.

Plan of Action and Milestones

OMB requires agencies to create and maintain POAMs for all known IT security weaknesses and report the status of the associated remedial actions to senior management on a quarterly basis. OMB also is explicit in what data it requires documented for each known security weakness.

Progress:
Management hired a CISO to oversee the security operations. In addition, management hired two additional Information Security Analysts in FY 2015 to assist with the administration of the IT security program. These resource's responsibilities include the maintenance of the security documentation, including the agency POAMs, and the oversight of remedial actions.

Issues to Be Addressed:	**Management Response:**
The OIG reviewed the CPSC's POAMs and found that Program Officials have not maintained and updated the agency's POAMs throughout FY 2015. Therefore, management does not actively track and maintain a list of security weaknesses and cannot provide an accurate quarterly report to the CIO on the progress of remediation efforts.	*EXIT does not concur with this finding. IT security team updated the POAM tracking list in FY2015 based on FY2014 audit findings. The IT security team also met with System Owners throughout FY2015 to review POAM status and update POAMs accordingly.*

All information required by OMB M-04-25 in the POAMs and the required information for all security weaknesses was not documented consistently.	*EXIT concurs. Several of the POAMs are missing milestone dates, Project Identifiers, funding sources, estimated cost/funding, responsible organization. This finding should be remediated through the use of the agency's new GRC tool.*
Management does not adhere to established remediation dates documented in the agency POAMs or provide adequate justification for missed remediation dates.	*EXIT Concurs.*

Recommendations:

1. Management should update existing POAMs to include the most recent information known and current status of each security weakness.
2. Management should actively maintain security documentation, including POAMs, for all major agency systems and brief relevant senior management on the changes. The CIO should validate the POAMs activities periodically (at least quarterly).
3. Management should document the key milestones for all security weaknesses tracked in the agency POAMs.
4. Management should document the dates associated with the key milestones for all security weaknesses tracked in the POAMs.
5. Management should document all changes to the milestones or milestone dates in the POAMs.
6. Security weaknesses documented in the POAMs, associated to investments identified in the IT Investment portfolio, should include Unique Investment Identifiers/Unique Project Identifiers to allow agency officials to trace the security weakness to the budget documentation.
7. Management should complete all POAMs fields for all security weakness.
8. Management should perform an assessment of the level of effort required for the remediation of each security weakness. The results of that assessment should be reflected in the milestone/milestone dates and "Estimated Completion Date" fields in the associated POAMs.

Continuous Monitoring

In an effort to ensure agencies develop processes for real time risk management and monitor their security posture on a continuous basis, OMB issued Memorandums and NIST Special Publications. In addition, on May 28, 2015, the Council of Inspector Generals on Integrity and Efficiency (CIGIE) released an Information System Continuous Monitoring (ISCM) maturity model. The purpose of the model is to: "*(1) summarize the status of agencies' information security programs and their maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and (3) help ensure consistency across the OIGs in their annual FISMA reviews.*" Using this guidance, we assessed the CPSC's ISCM program to determine the agency's current ISCM maturity level. We determined that the CPSC has achieved level one in each of the domains (people, processes, and technology).

Progress:

Management has reviewed and updated the ISCM Policy, ISCM Strategy, and ISCM Risk Assessment in FY 2015 to facilitate compliance with FISMA requirements. The ISCM strategy included the list of security controls employed, security control testing frequencies, and schedules. The ISCM strategy also included the list of security metrics monitored, their assessment, and reporting frequencies. Management received periodic ISCM metric status reports, reports on the results of ongoing assessments, and remediation efforts to assist with risk management. This process will continue to improve as management implements new monitoring tools and optimizes its existing tool set. Management intends to have the program fully implemented by 2017, as part of the phased approach described in OMB M-14-03.

Issues to Be Addressed:	**Management Response:**
Management did not adequately define the ISCM stakeholders and communicate their responsibilities across the organization. Roles and responsibilities are defined within the ISCM policy and strategy documents, however: – management did not communicate the ISCM policy/plan to the requisite business/mission resources; and – the Risk Executive Function was discussed in the ISCM Plan, but was not included in the Roles and Responsibilities section of the ISCM Policy. Additionally, the establishment of Risk Executive Function has not occurred.	*Management was provided an opportunity to respond to this finding and did not.*

Management did not perform a skills, knowledge, and resource "Gap Analysis" to identify and remediate the missing security program capabilities necessary to implement and support the agency's ISCM strategy. The ISCM Gap Analysis performed did not include recommendations for the types of skills/knowledge (training) required to implementing the agency's ISCM strategy or the solutions involved with implementing this strategy. This is due to the timing and scope of this assessment. According to the purpose section of the Gap Analysis, the ISCM strategy skills, knowledge, and resource gap assessment was to "determine the gap between what is required and current CPSC ISCM capabilities" and thus, not in scope for this report. In addition, the completion of the ISCM Plan/Strategy did not occur at the time of the performance of Gap Analysis.	*EXIT concurs with the finding and will update its ISCM Gap Analysis in FY16 to provide a more current assessment of EXIT skills, knowledge, and resources required to successfully implement and maintain ISCM. EXIT will also develop a remediation strategy to addresses ISCM deficiencies related to skills, knowledge, and resources.*
The CPSC ISCM plan states that management requires a full system reauthorization when an "event occurs that produces risk above an acceptable organizational risk tolerance—such as a catastrophic breach/incident or significant problems with the ISCM program." However, management has not defined the methodology used to calculate the agency's Organizational Risk Tolerance, developed an Organization-Wide Risk Management Strategy, or established a Risk Executive Function. Therefore, the OIG cannot assert that the risk tolerance stated in the ISCM plan is based on the actual risk the organization as a whole is willing to accept in pursuit of its goals and objectives. In addition, the OIG does not believe the best course of action is to wait for an issue to arise, especially a catastrophic breach/incident, before management considers reauthorizing a major agency system, as is suggested in the agency's ISCM risk tolerance statement.	*EXIT agrees with the finding that the ISCM strategy has not been integrated with agency risk tolerance requirements. An agency-wide risk tolerance strategy has not been developed. Therefore EXIT has adopted an alternative approach to managing information system risk. The ISCM strategy utilizes Cross-Agency Priority Goals, ISCM related policy memoranda, and/or annual FISMA metrics to help establish risk tolerances.* *EXIT also utilizes several other sources for managing risk, such as threat intelligence sources, knowledge of threat tactics, techniques, and procedures, private and public sector information sharing organizations, and hardware/software vendors. New risks which merit monitoring and response are discovered on a regular basis. EXIT is proactive in identifying threats and vulnerabilities in order to improve the quality of its risk management capabilities and to have the most impact on actually reducing risk.*

	EXIT has adopted "ongoing" authorization for its critical information systems—which allows an organization to replace a static, point-in-time security assessment and authorization process with a dynamic, near-real-time (ongoing) security assessment and authorization process.
Management has not performed a BIA, communicated the ISCM policy and strategy to mission stakeholders, or included the mission stakeholders in the performance of the ISCM Risk Assessment. Therefore, management did not adequately consider mission and business requirements and impacts when developing the ISCM strategy.	*Management was provided an opportunity to respond to this finding and did not.*
Management has not fully defined the following ISCM processes: hardware asset management, software asset management, and data collection requirements for defined security metrics and reporting.	*EXIT concurs with the finding and will update its ISCM plan in FY16 to incorporate specific procedures on how it will address hardware asset management, software asset management, and data collection requirements for defined security metrics and reporting.*
Management suggested that the metrics show the effectiveness of the ISCM program by highlighting areas of focus and concern within the agency's security posture. The metrics management defined in the ISCM strategy provides management with situational awareness into the areas designated. However, the metrics do not provide insight into the effectiveness of the ISCM program itself. An example of a metric that would provide this insight would be assessing the length of time that malware remained undetected on the network.	*EXIT concurs with the finding and will review its ISCM program to identify appropriate metrics to help gauge the effectiveness of its ISCM program.*
Management has not developed lessons learned from the ISCM program to identify areas of potential improvement. Also, management has not defined a process to capture the lessons learned associated with the agency's ISCM program.	*EXIT concurs with the finding and will review its ISCM program to identify practices that can be used to help capture and share lessons learned related to the effectiveness of ISCM processes and activities.*
The CPSC has not identified, fully defined, and planned for the ISCM technologies needed in the following automation areas of the ISCM program: – License management	*EXIT concurs with the finding and will update its ISCM plan to identify and fully define the technologies it plans to utilize to automate ISCM activities.*

– Information management – Software assurance – Asset management – Network management	
The CPSC has not defined how it will use automation to produce an accurate point-in-time inventory of authorized and unauthorized devices and software on its network; as well as, the security configuration of these devices and software.	*EXIT concurs with the finding and will update its ISCM plan to identify and fully define the technologies it plans to utilize to automate point-in-time authorized/unauthorized hardware/software inventories.*

Recommendations:

1. Management should define the responsibilities for all ISCM stakeholders and communicate this information to those resources. These resources must include mission/business representatives and those involved with the Risk Executive Function, as described in the ISCM policy/strategy documents.

2. Management should perform a Gap Analysis to identify the missing skills, knowledge, and resources required to implement the ISCM program.

3. Management should develop a remediation plan for each of the shortfalls noted in the ISCM Gap Analysis.

4. Management should implement the remediation plan, noted above.

5. Management should periodically reassess the ISCM program for skills, knowledge, and resource gaps as the ISCM process matures.

6. Management should clearly describe the methodology used to calculate the organizational risk tolerance and include this description in the Organization-Wide Risk Management Strategy.

7. Management should then integrate the organizational risk tolerance to described in the Organization-Wide Risk Management Strategy into the agency’s ISCM strategy.

8. Management should perform a BIA.

9. Management should update the ISCM program based on the BIA.

10. Management should integrate mission/business resources into the ISCM process.

11. Management should update the ISCM policy/strategy or develop SOPs to document how it plans to perform hardware/software management and how it plans to collect the security information required for the metrics outlined in the ISCM strategy. The data collection techniques should include how the data is collected (tools used), what data is collected (content/scope), and how often is it reported.

12. Management should define and assess metrics that provide insight into the effectiveness of the CPSC's ISCM program.

13. Management should formally define and implement a process that facilitates consistently capturing and sharing the lessons learned related to the effectiveness of ISCM processes and activities.

14. Management should identify, fully define, and develop a plan for implementing the ISCM technologies it expects to utilize in the following automation areas:
    - License management
    - Information management
    - Software assurance
    - Asset management
    - Network management

15. Management should define how it plans to use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

Contingency Planning

FISMA requires that management develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Additional Federal standards and guidance for this processes is developed and disseminated by the Federal Emergency Management Agency (FEMA) and NIST.

Progress:
Management has not made any additional progress in this process in FY 2015. However, management is reviewing cloud technology solutions to remediate these issues and expects to begin performing these tasks in 2016.

Issues to Be Addressed:	**Management Response:**
The Contingency Planning Policy was not updated prior to the OIG cutoff date on September 20, 2015, and management has not enumerated all of the TT&E program requirements defined in FCD1 in this policy.	*EXIT does not concur*.
Management has not implemented the CPSC Contingency Planning Policy. As such, management has not: – developed a current and formal BIA; – established, documented, formalized or tested a DR Plan, BCP, or COOP; – established, formalized or tested ISCPs for all agency systems; – reviewed and updated the all of the agency's existing ISCPs in FY 2015; and – established an Alternative Processing Site.	*Concur*.

Management does not employ backup strategies to meet the Recovery Point Objectives (RPOs) documented in the ISCP. Specifically, the RPOs documented in the CPSC ISCP cannot be achieved with the management's current backup schedules.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

Recommendations:
1. The CPSC should develop and implement an FCD1 compliant TT&E program and include those program requirements in an updated Contingency Planning Policy. 2. Management should train all of the relevant resources on the continuity planning responsibilities assigned to them in the policy. 3. Management should perform, document, and approve a formal BIA in accordance with NIST SP 800-34. 4. Management should establish, document, test, and approve a DR Plan, BCP, and COOP. 5. Management should establish, formalize, test, and approve ISCPs for all critical agency systems in accordance with FEMA guidance. 6. Management should document an RPO for all relevant agency systems. 7. Management should implement a solution to allow management to meet the documented RPOs for all relevant systems. 8. Management should draft After-Action Reports to document the "lessons learned" identified as part of the COOP, DR Plan, and BCP testing. 9. Management should establish an alternative processing site. This site should contain the equipment and supplies required to recommence operations in time to support the organization-defined time period for resumption. 10. Management should train all relevant resources on the continuity planning responsibilities assigned to them in the policy.

Contractor Systems

Per FISMA, Section 3544(b), agencies are required to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.” This includes services that are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions. To this end, management must develop and maintain an inventory of the CPSC’s IT systems hosted by third parties. Management also must develop policies to govern this process, and use contracts, Service Level Agreements (SLAs), Memorandums of Understandings (MOUs), and/or Inter-Agency Service Agreements (ISAs) to govern all inter-governmental and non-governmental IT relationships.

Progress:
Management has not made any additional progress in this process in FY 2015.

Issues to Be Addressed:	**Management Response:**
The Contractor Security Oversight policy was not reviewed or updated in FY 2015 and is missing the following information: – The process by which management controls cloud-based SaaS implementations – A requirement for management to assess all third party systems' compliance with FISMA and accredit the operation of each third party system in the CPSC environment. – The frequency that management must review/update agency MOUs/ISAs.	*EXIT concurs. Policy needs to be updated.*
The Contractor Security Oversight Policy is not fully implemented: – Management has not established processes and procedures to track various ISAs and metrics applied throughout the lifecycle of the third party IT security services within the CPSC; – Management does not notify third parties of intrusions, attacks, or internal misuse, so the third party can take steps to	*EXIT concurs. Policy needs to be updated.*

determine whether its system has been compromised; – Management does not analyze audit logs to detect and track unusual or suspicious activity across the interconnection that might indicate intrusions or internal misuse; – Management does not use automated tools to scan for anomalies, unusual patterns, and known attack signatures across the interconnection and to alert administrators if a threat is detected; – The ISSO or delegate does not periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize; – Management does not coordinate contingency planning, training, testing, and exercises with any third party contractors to minimize the impact of disasters; and, – Management has not established joint procedures with third parties based on existing contingency plans.	
Per CPSC's 3rd Party IT Systems Inventory document, the CPSC currently connects to eight remote systems hosted by third Parties. However, during our review of the ISA/MOUs agreements for the eight systems identified, management was unable to provide signed and current ISAs for six of the third party systems.	*EXIT concurs. The new GRC tool has functionality that will help remediate this finding. The new tool has the ability to notify key personnel when agreements are approaching expiration dates.*
Management has not assessed the security controls associated with the third party systems that connect with the CPSC network.	*EXIT does not concur with this finding. The FISMA metric associated with this finding attempts to determine if the agency obtains sufficient assurance that the security controls implemented by third party systems are implemented effectively and compliant with FISMA requirements. Management has determined that a valid authorization to operate for a third party system provides sufficient assurance of effective and compliant control implementation. The audit recommendations for this finding are impractical and unsustainable as they would more than double the resources required for the agency's IT security staff and would not produce a corresponding reduction in overall*

	agency risk.
The 3rd Party IT Systems Inventory is incomplete.	*EXIT concurs.*

Recommendations:

1. Management should update the Contractor Oversight Policies and Procedures to include the following:
   - The process by which cloud-based SaaS implementations are controlled.
   - A requirement for management to assess all third party systems' compliance with FISMA and to accredit the operation of each third party system in the CPSC environment. In order to ensure that all security controls are implemented and operating effectively management must assess all related user controls. Management should use the results of this assessment, in combination with the results of third party's assessment of its security controls, as a basis to accredit these systems. Management should also develop procedures to guide this process.
   - The frequency that management must review/update agency MOU/ISAs.

2. Management should establish processes and procedures to track the various ISAs and metrics that management applies throughout the lifecycle of a contract.

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 notify connecting third parties of known security weaknesses that might have an impact on the third parties systems.

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 across the interconnection; and, management should configure these tools to alert administrators of detected threats.

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

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

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

10. Management should establish a current ISA with all third parties that interface the CPSC network.

11. For each of the third party solutions, management should identify all controls the agency is responsible for implementing.

12. Management should develop an SSP for each of the third party solutions based on the above-described assessment or update existing security plans to include this information.

Configuration Management

According to FY 2015 metrics, a key goal of configuration management is to make assets harder to exploit through better configuration. In order for this to be effective, the configuration management process must be complete, accurate and operate in near real-time. To this end, agencies are required to implement and monitor agency compliance with USGCB (formally, the Federal Desktop Core Configuration) and to document and implement configurations for all agency systems listed in the NVD.

Progress:
Although management has not implemented Defense Information System Agency (DISA) configuration settings to all agency systems, management has made significant progress in this endeavor. Management implemented a whitelisting solution on agency clients on June 30, 2015 and plans to implement this solution on its servers in FY 2016. In an effort to improve its ability to restrict unauthorized client software from executing on the network, management implemented a formal review over local administrator rights to workstations and has implemented a systematic process to remove existing local administrative privileges on a daily basis. Further, management has restricted the ability of telework clients to directly access the internet (split tunneling) at the time of our testing in September 2015. Management also is in the process of restricting split tunneling for clients that are not typically used for telework. The CPSC has further improved and continues to improve its automated scanning capabilities, even though the results of these scans were not consistently reported to senior management. In addition, management improved its patching processes in response to the OMB's "30 day Sprint." However, management still has not applied all requisite patches or established a process for the timely patching of all agency systems. Further, management now requires all changes to undergo a formal Security Impact Assessments prior to implementation. These enhancements will, among other things, reduce the agency's attack surface, assist management in detecting/preventing attacks, reduce the amount of unauthorized software on the network, improve software license compliance, and reduce the effort required to develop a comprehensive software inventory.

Issues to be addressed:

Issues to Be Addressed:	**Management Response:**
Management did not update the Configuration Management Policy prior to the OIG cutoff date on September 20, 2015 and the following information was not included in the policy: – The frequency with which management must review/update the Configuration Management Policies and Procedures. – A description of organization-defined circumstances when management must update baselines or an explicit requirement for updating baselines as an integral part of information system component installations and upgrade. – A requirement for management to develop and document an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability; or a requirement that management reviews and updates the information system component inventory within an organization-defined frequency. – A requirement for management to take action when unauthorized components are detected. These actions should include one or more of the following: disabling network access to such components; isolating the components; notifying organization-defined personnel or roles. – In addition, management has not developed Configuration Management procedures. The link within the policy that references the Configuration Management procedures is broken.	*EXIT does not concur*.
Management has not fully implemented the Configuration Management Policy. We identified that management: – Has not documented and formally accepted the variances from the NVD provided by the Security Technical Implementation Guides (STIGs) in accordance with NIST SP 800-53 CM-6. In addition, management does not scan all servers for DISA	*Concur*.

non-compliances. – Does not remediate DISA non-compliances identified in all scans within the 30 days, as required by the Configuration Management Policy. – The policy refers to SOPs, although management has not fully developed or implemented these SOPs and the link within the policy is broken.	
Management has not developed and maintained a comprehensive inventory of software and hardware or developed a process to ensure software licensing compliance.	*Concur*.
Management has not developed an inventory of software and hardware components requiring configuration baselines; and has not baselined all agency software and hardware component configurations.	*Concur*.
Management has not applied all USGCB settings to agency clients or documented and formally accepted all variances from the USGCB settings. Management did not consistently perform scans to identify USGCB non-compliances in FY 2015. In addition, management does not remediate the unauthorized variances identified in the scans within the timeframes outlined in the agency policy.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*
Management permits external connections to flow through a non-Managed Trusted Internet Protocol Services (MTIPS) connection, as is required by the Trusted Internet Connection (TIC) initiative.	*Concur*.
Management has not consistently performed scans to identify missing patches/vulnerabilities and USGCB/DISA non-compliances. Management did not perform these scans in October 2014, November 2014, December 2014, April 2015, and May 2015.	*Concur*.
Management does not implement server, database, and widely-used third party application patches in a timely manner. Also, management does not document the test steps taken in the change control forms. Additionally, management is using versions of	*Concur*.

databases that the vendor no longer supports.	
Management has not selected/documented/implemented the baseline configuration settings for all systems described in the NVD, in accordance with NIST SP 800-53 CM-6 and NIST SP 800-70.	*Concur.*

Recommendations:

1. Management should review and update the Configuration Management policies, and develop and implement SOPs to standardize the implementation of the Configuration Management process. The Configuration Management policy/SOPs should include the following:
    a. A description of organization-defined circumstances when baselines must be updated or an explicit requirement for baselines to be updated as an integral part of information system component installations and upgrades.
    b. A requirement for management to develop and document an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability; or a requirement that management reviews and updates the information system component inventory within an organization-defined frequency.
    c. A requirement for management to take action when unauthorized components are detected. These actions should include one or more of the following: disables network access by such components; isolates the components; notifies organization-defined personnel or roles.
    d. The frequency in which management must review/update the Configuration Management Policies and Procedures.

    Also, management should document configuration management SOPs, and update the policy to include an accurate reference to those procedures.

2. Management should formally document and configure all agency systems according to the STIGs described in the NVD.

3. If a configuration in a STIG cannot be applied for a legitimate reason, management should formally document the reason.

4. Management should scan all agency systems for compliance with the organizationally selected hardening guides.

5. Management should remediate all unacceptable deviations identified in the DISA scans within 30 days, as outlined in the Configuration Management Policy.

6. The agency should implement a solution to develop, approve, and maintain a current and comprehensive software/hardware inventory.

7. Management should then assign ownership to all agency software/hardware.

8. Management should develop, approve, and maintain a target software/hardware inventory.

9. Purge the network of all unauthorized software.

10. Implement a process to scan the network to identify any unauthorized software/hardware on the network. This may be achieved through the DHS Continuous Diagnostics and Monitoring (CDM) program.

11. Patch all software identified in the authorized software inventory.

12. Develop and enforce a process to govern software license compliance:
    a. Document a comprehensive software inventory.
    b. Document how many instances of each type of software are installed on the network.
    c. Document an inventory all software licenses owned by the agency.
    d. Reconcile the software instances installed on the network to the software licenses owned by CPSC and remediate any discrepancies.

13. Perform periodic audits to ensure future compliance.

14. Management should develop an inventory of components 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.

15. Management should establish and document mandatory configurations and configuration settings for information technology products employed within the information system. The configuration settings (CM-6) should use defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

16. Management should then implement the identified configuration settings.

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

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

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

20. Management should review/update the existing configuration baselines each time a major change is made to the system's environment and, at least annually.

21. Management should formally document and configure all agency systems according to the USGCB setting checklists, including the Microsoft Solutions for Security Settings (MSS Settings).

22. If a USGCB configuration cannot be applied for a legitimate reason, management should formally document the reason.

23. Management should implement the TIC for all external connections.

24. Management should perform scans to identify missing patches/vulnerabilities and USGCB/DISA non-compliances on a monthly basis and remediate the vulnerabilities/non-compliances identified according to the timeframes outlined in the agency policy.

25. Management should implement client, server, database and widely used application patches in a timely manner and in accordance with the patch management policy. If the agency decides not to implement the missing patch, management should document a formal justification.

26. Management should test all client, server, database, and application patches in a test environment prior to deploying the patch to the full production domain.

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

28. Management should add a separate query to the change management database to allow users to search on server, database, and

application patches.

29. Management should upgrade to a supported version of SQL, or migrate to another supported database.

Incident Response and Reporting

NIST requires management to establish incident detection, handling, and analysis policies and procedures. Additionally, management is required to notify the United States Computer Readiness Team (US-CERT) of security incidents in accordance with the US-CERT Concept of Operations requirements.

Progress:
Management has made substantial progress in improving Incident Response and Reporting in FY 2015. Management has implemented the Incident Response policies and procedures and reports incidents to US-CERT in a timely manner. The CPSC's CSIRT is proactive in its approach to identifying and resolving incidents and has improved its solutions profile sufficiently within the past year to facilitate this proactive approach. In addition, as the CSIRT gains experience and incident response solutions improve, the CPSC is becoming more efficient and effective at detecting and resolving security incidents.

Issues to Be Addressed:	**Management Response:**
Management has defined goals and metrics for the timely resolution of security incidents. However, due to the incident response form used by the CPSC not requiring the recording of the date and time that security incidents are resolved, the OIG was unable to determine whether some of the incidents were resolved in a timely manner.	*The IT security team responded to a number of cyber incidents during the past year and proactively identified and contained various malware attacks. Very often, after an attack had been identified and contained, IT security opened a Helpdesk ticket to have the infected system removed, reimaged, or re-scanned. The actions taken by the Helpdesk were not always date/time stamped in a manner that supported after-the-fact auditing of incident response times. In order to address this deficiency the IT security team will explore the possibility of integrating its incident tracking processes with the agency Helpdesk tracking system. The IT security team will create and manage incident tickets and associated milestones, including closures, throughout the entire incident lifecycle—utilizing the agency Helpdesk system.*

Recommendation:
1. Management should update the Incident Response Form to require the date and time of the incident resolution, and provide sufficient information in the Incident Report to allow the reader to understand the steps taken to resolve the issue.

Security Training

NIST and the Code of Federal Regulation (C.F.R) require the CPSC to provide Security Awareness Training and role-based trainings to all employees/contractors who have significant information system security responsibilities.

Progress:
Management obtained role based training courses from the Veterans Administration and provided these trainings to EXIT users management identified as having significant security responsibilities. In addition, in FY 2015, management provided role-based training to program managers, IT Specialists and executives in an effort to comply with 5 CFR 930.301. Management is planning on customizing the role based training in FY 2016 to reflect the CPSC's policies, procedures, processes, and to meet the requirements of 5 CFR 930.301.

Issues to Be Addressed:	**Management Response:**
The Security Training Policy does not require role-based training for non-IT staff, including those explicitly outlined in the 5 C.F.R 930.301. Instead, management has decided to "tailor-out" all users with significant security responsibilities that are not EXIT system administrators.	*The Security Training Policy in question is an "EXIT" policy and it mandates role-based training for specific IT roles (within EXIT) that have significant system security responsibilities—these include: IT security, system administration, database administration, network architecture, application development, website administration, data backup/recovery, email administration, or firewall administration. This training is an annual requirement. The statute referenced in the audit finding is a broad requirement which addresses security training for various non-IT roles, such as executives, program managers, auditors, etc. Because of the high-level nature of this training it appears that this finding is more of a personnel matter rather than an IT deficiency*
The agency does not provide role-based training to all the personnel who require this training:	*The Security Training Policy in question is an "EXIT" policy and it mandates role-based training for specific IT roles (within EXIT)*

– Role based training was not provided to non-IT users, such as executives, in information security basics and policy level training in security planning and management as is required by NIST SP 800-53, AT-3 and 5 C.F.R 930.301. – Application security officers/administrators were not provided "training in information security basics and broad training in security planning, system and application security management, system/application life cycle management, risk management, and contingency planning." as is required by NIST SP 800-53, AT-3 and 5 C.F.R 930.301. – Role-based training was not provided to all contractors with significant security responsibilities. In addition, the role-based training provided was not customized to reflect the CPSC's processes, policies, and procedures.	*that have significant system security responsibilities—these include: IT security, system administration, database administration, network architecture, application development, website administration, data backup/recovery, email administration, or firewall administration. This training is an annual requirement. The statute referenced in the audit finding is a broad requirement, which addresses security training for various non-IT roles, such as executives, program managers, auditors, etc. Because of the high-level nature of this training it appears that this finding is more of a personnel matter rather than an IT deficiency.*

Recommendations:

1. The agency should update the Security Training Policy and develop a 5 C.F.R 930.301 compliant training program, using the guidance outlined in NIST SP 800-16 and NIST SP 800-50:
   – The Security Awareness and Training policies and procedures should require management to provide each relevant NIST SP 800-16 defined "user group," security training specifically developed for their role within the agency. This should even include resources outside of IT.

   Management should also outline the training criteria, if not the content, for each user group 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 applicable agency resources to one (or more) of the relevant user groups mentioned above as required by NIST SP 800-16/50 and C.F.R 903.301.

3. Once management has assigned each of the relevant users to a user group, management should provide those resources the associated training(s).

Remote Access Management

NIST requires management to establish and implement Remote Access Policies and Procedures. The 2004 Homeland Security Presidential Directive (HSPD) 12 compels agencies to require the use of Personal Identification Verification (PIV) Cards as the common means for the majority of standard users to access the network remotely. In addition, OMB compelled agencies to implement the Trusted Internet Connection (TIC) to assist with the government-wide effort to consolidate external network connections across the Federal landscape in 2008.

Progress:

On August 26, 2015, the CPSC began a systematic requirement for PIV cards to access agency clients unless a compelling justification existed for circumventing this control. As a complementary control, management identifies users who did not authenticate using a PIV card to detect and remediate non-compliances with the NIST and HSPD-12 mandates. This process partially remediates the risk associated with users who remotely access agency systems without multifactor authentication. In addition, management has implemented a Privileged User Management Solution to manage privileged access and to eliminate the use of common administrator accounts. Management expects full implementation of the solution in FY 2016.

Issues to Be Addressed:	**Management Response:**
The Remote Access policies and procedures are out-of-date and management did not review and update these documents in FY 2015. In addition, these policies and procedures are missing key elements: – The policy does not define all authorized methods of remote access. – The policy does not include usage restrictions, configuration/connection requirements, and implementation guidance for each remote access method. – Management has not documented how they monitor all forms of remote access. – Management has not documented the list of privileged/security functions and security-related information that users can access remotely, organizational requirements/needs to grant this access, or the additional controls in place to ensure these functions are not misused.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

– Management has not defined the networking protocols the agency has deemed non-secure within the policies/procedures.	
Further, management has not fully implemented the remote access policies and procedures, as management: – Does not monitor all remote connections for unauthorized access or misuse; – Requires the use of FIPS 140-2 in the Secure Communication Policy. However, management has not implemented FIPS 140-2 solutions for remote access and does not systematically require encryption for information transmitted across public networks. For example, management has not configured the CPSC email solution to systematically encrypt, emails and attachments prior to transmission across a public network; – Utilizes a Non-MTIPS internet connection; – Does not systematically prohibit split tunneling; – Does not document situations or compelling reasons to grant remote access to privileged commands or access to security-related information; – Has not reviewed the Remote Access policy since 2012, but documented an annual review in the Remote Access Policy; and – Has not developed a traffic flow policy, as required by the System and Communication Protection Policy.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*
Management does not require all devices to authenticate to the network or formally authorize and document a list of devices/types of devices that must authenticate to the network.	*Concur.*
The CPSC's CSIRT was not notified of all instances of missing laptops/Blackberries in FY 2015. Therefore, management was not able to make a timely determination regarding if these devices contained sensitive information or were adequately disabled/encrypted/reported. In at least some instances, CSIRT was first notified about missing devices by the OIG as a byproduct of the FISMA review.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

Recommendations:

1. Management should document and implement the following processes in a policy or procedure document:
    - An inventory of authorized methods of remote access.
    - Usage restrictions configuration/connection requirements and implementation guidance for each remote access method.
    - The list of privileged/security functions and security-related information that users can access remotely, organizational requirements/needs to grant this access, and the additional controls in place to ensure these functions are not misused.
    - Specific audit procedures for each remote access method to ensure these controls are in place and effective.
    - An inventory of networking protocols management deems non-secure and a requirement to restrict access to these protocols.
    - An inventory of organization-defined devices/types of devices, which require unique identification and authentication before establishing a local/remote/network connection.

2. The CPSC should follow the documented organizational policy and the NIST requirements. These requirements include the implementation of automated tools to monitor for unauthorized remote access connections and the misuse of authorized remote access connections. Management should also report the results of these analyses to all appropriate parties.

3. Management should implement FIPS 140-2 validated encryption solutions for all forms of remote access.

4. Management should implement a solution to require systematically the encryption of all sensitive information transmitted across a public network. Otherwise, management should audit periodically e-mails, attachments, and file transfers traversing a public network to ensure policy compliance. Alternatively, management should implement a data loss prevention solution.

5. Management should prohibit split tunneling systematically and route all traffic through the Trusted Internet Connection

6. Management should define, document, and authorize all instances where remote access to privileged commands and security-related information is granted.

7. Management should perform an annual review of the remote access policies and procedures.

8. Management should document a traffic flow policy.

9. Management should implement a Network Access Control device that requires the Institute of Electrical and Electronics Engineers

Standards Association (IEEE) 802.1x authentication for all CPSC devices (including network devices, servers, and printers) prior to granting access to the network.

10. Management should update the Property Management policies and procedures to require Property Custodians to notify the ISSO/CSIRT of missing devices that may contain CPSC data (e.g. flash drives, external hard drives, desktops, servers, laptops, Blackberries, etc…) as soon as these devices are identified.

11. Management should train all Property Custodians on their responsibility to notify the ISSO/CSIRT immediately when they become aware of lost or stolen devices that may contain CPSC data.

12. Management should hold users accountable for not reporting missing devices that may contain CPSC data immediately upon discovery.

Identity and Access Management

NIST requires agencies to establish physical and logical access policies and procedures to govern identity and access management processes. In addition, DHS compels agencies to establish the use of PIV cards as the common means for standard users to access agency facilities and log into agency clients.

Progress:
On August 26, 2015, management began systematically requiring most users to utilize multifactor authentication to access agency clients. Management also began formally documenting, tracking, and monitoring all clients that do not require multifactor authentication. In addition, management established a formal process to authorize privileged access requests and requests to establish new-shared network accounts in FY 2015. Lastly, management performs periodic audits of network accounts to identify inappropriate users.

Issues to Be Addressed:	**Management Response:**
Management did not review and update the General Access Control Policy in FY 2015. In addition, management did not document the following AC-1 and AC-2 requirements in the General Access Control policy and related procedures: – How often management reviews/updates the access policies	*Concur. Policy was updated in 2015 but is currently in a draft format undergoing revisions.*

and procedures; – Conditions established for role/group membership, – Account modification procedures; – The process for reissuing shared/group account credentials when individuals are removed from the group; – The process by which management controls system accounts; and – References to individual system access control SOPs and the shared and privileged account request authorization access control SOPs.	
The user access control procedures were not reviewed or updated in FY 2015. In addition, management did not document the following AC-1 and AC-2 requirements in the user access control procedures: – CPSRMS o How often management reviews/updates the access procedures, o Account modification procedures, o Frequency of user account reviews, and o References to General Access Control Policy. – Dynamic Case Management (DCM) o How often management reviews/updates the access procedures, o How management establishes a proper segregation of duties and the principle of least access within the application, o The process by which management establishes and controls common accounts, o Account modification procedures, o A requirement for the periodic review of user access, and o References to General Access Control Policy. – Cpsc.gov	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

o Procedures do not exist.	
Management has not fully implemented the General Access Control policy, as follows: – CPSC ITTS Branch Chief and Program Managers do not assess access controls for all users with administrative and non-administrative access privileges on an annual basis, as Management does not: o Maintain a list of all security systems and security controls in place for each system; o Maintain a description of the processes by which users are granted access to each system; o Audit all users with access to CPSC systems and confirm group access settings are accurate. – Management utilizes shared administrative accounts.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*
Management does not utilize separate accounts for administrators. Instead administrators utilize privileged accounts to perform non-privileged tasks.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*
The CPSC has not implemented the Principle of Least Privilege and proper segregation of duties for the GSS LAN. The CPSC does not have the ability to report-on/track users with access to specific security functions within Active Directory (AD) or E-Directory. Since the agency has not implemented a solution, which will allow them to develop reports with this level of granularity, the Principle of Least Privilege cannot be ensured. In addition, management does not define conditions for group/role membership. If a user is granted administrator access to the GSS LAN, he/she can perform all security functions instead of being granted access to only those functions required by the	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

user's job responsibilities. This results in users that are granted access rights that exceed their job responsibilities. Additionally, administrators have sufficient access to access and alter the audit logs.	
Management has not implemented the Principle of Least Privilege or Segregation of Duties within cpsc.gov. There are 31 individual users (including one student trainee) and five common accounts with sufficient access to author and publish content to cpsc.gov without further review or approval.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*
Management does not periodically review all common accounts for appropriateness or to change the passwords for these accounts, as business needs require. For example, once a user of a common account separates from the agency or changes job functions and no longer requires access to the account, management should change the common account's password.	*EXIT does not concur.*
Management does not document and maintain the time and date the agency revokes network accounts. Therefore, management cannot evidence the timeliness of all network access revocations. In addition, we identified 19 specific incidents where management did not immediately disable/remove agency information system accounts upon contractor/employee/volunteer separation from the agency. However, please note that in all but five of these 19 incidents the users' network accounts were disabled, substantially limiting the risk of compromise. In addition, less than 0.9% (5 in 683) of network enabled accounts were assigned to a user whom had separated from the agency.	*Not enough time allotted to research and provide a meaningful response.* *OIG Rebuttal: Management indicated that they did not have adequate time to respond this finding. However, when management was asked how much additional time they would require they failed to respond.*

Recommendation:
1. We recommend that management include the following elements in the General Access Control Policy and procedure documents: – How often management reviews/updates the access policies and procedures.

- The process by which common network accounts are controlled. This should include, conditions established for group membership, how common/anonymous accounts are monitored, and how shared credentials are reissued when individuals are removed from the group.
- Account modification procedures.
- The process by which the agency establishes and controls system accounts.
- References to individual system access control SOPs and the shared and privileged account request authorization SOPs.

2. Management should document user access control procedures for all agency systems, where applicable, and the existing user access procedures. Thus, we recommend that Management include the following elements in all user access control policies and procedures:
   - How often management reviews/updates the access procedures.
   - Account modification procedures.
   - A requirement for the periodic review of user access included in all of the procedure documents along with detailed procedures describing how these reviews are performed.
   - A description of how management implements the principle of least access and segregation of duties.
   - The process by which common accounts are established and controlled. This should include how common/anonymous accounts are authorized and monitored and how shared credentials are changed when individuals are removed from the group.
   - A reference to individual system access control SOPs in the General Access Policy; as well as, a reciprocal reference in the General Access Policy to the user access control procedures.

3. Management should ensure that the General Access Control Policy is fully implemented. We recommend that Management assess access controls for all users with administrative and non-administrative access privileges on an annual basis. This includes requiring that:
   - Management maintains documentation to include a list of all security systems and security controls in place for each system.
   - Management maintains an up to date list of the process by which users are granted to each system.
   - Management audits all users with access to CPSC systems and confirms group access settings are accurate.
   - Management should not utilize shared administrator accounts.
   - Management ensures that all Access Control policies and procedures are disseminated to all resources with significant access control roles and responsibilities.

4. 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.

5. 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.

6. Management should implement the Principle of Least Privilege and proper segregation of duties for the GSS LAN.
    - The agency should define and document the functions/duties, which have a significant impact on agency operations and assets and create roles that systematically separate the users' ability to perform these functions.
    - The agency should revoke access to all users who have, but do not require access to, the functions defined above.
    - 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.
    - The agency should document the system controls in place (e.g., blocked ports, restricted protocols, etc.).
    - 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.).
7. Management should implement a solution, which 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.

8. 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.

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

10. Management should implement the Principle of Least Privilege and proper segregation of duties for cpsc.gov, as follows:
    a. The agency should assign privileges that coincide with the defined roles within cpsc.gov. These roles should be defined in a Segregation of Duty Matrix within a cpsc.gov user access SOP.
    b. Management should develop and implement automated workflows within cpsc.gov to coincide with the roles defined within cpsc.gov. The workflow should require the approval of all published web content systematically from an organization-defined, separate, independent, and appropriate resource.
    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.

11. Management should perform periodic audits of user access to ensure access remains appropriate.

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

13. We recommend that management implement a formal process:
    - To establish and control the use of shared user accounts.
    - To disable common user accounts once no longer required.
    - 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.
    - To 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.
    - 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.
    - To require periodic password changes on all common accounts.
    - To require periodic review of all common user accounts to ensure these accounts remain appropriate

14. Management should revoke the separated users' access to the relevant information systems.

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

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

17. Management should train the Contractor Officer Representatives, Office of Resource Management (EXRM), and EXIT resources responsible for processing contractor separations on their respective contractor separation responsibilities.

18. Management should train all CPSC resources that manage volunteers on the CPSC off-boarding process.

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 Access Control Lists to ensure the timely revocation of all user accounts

APPENDIX A: BACKGROUND

Background

On October 30, 2000, the President signed into law the 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 FISMA, as revised in 2014, along with additional guidance from the Department of Homeland Security (DHS) lays out a framework for annual IT security reviews, reporting, and remediation planning. The FISMA seeks to ensure proper management and security for information resources supporting Federal operations and assets. The Act requires Inspectors General to perform an annual independent evaluation of their agency's information systems security programs and practices.

To establish a baseline to help it meet the requirements outlined above, the CPSC's OIG performed an independent review of the CPSC's automated information security control procedures and practices in FY 2015. The requirements of the review included:

- Evaluating and testing the internal controls defined in the 2015 FISMA metrics (provided by DHS);
- Testing the information security controls defined in the 2015 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 2015 FISMA metrics;
- Recommending improvements, where necessary, in security record keeping, internal security controls, and system security; and
- Identifying the degree of risk associated with identified internal security controls weaknesses.

APPENDIX B: OBJECTIVES, SCOPE, & METHODOLOGY

Objective

The objective of this review was to determine whether the CPSC complies with FISMA and has developed adequate effective information security policies, procedures, and practices. Additionally, the OIG evaluated the CPSC's progress in developing, managing, and implementing its information security program.

Scope

To accomplish our objective, our evaluation focused on the CPSC's information security program, the FY 2015 FISMA reporting metrics developed by DHS dated June 19, 2015 and the related requirements outlined by OMB, DHS, NIST, the Department of Commerce, FEMA, and the Federal Chief Information Officer Council. We conducted our evaluation from July 2015 to October 2015 at the CPSC's headquarters, located in Bethesda, Maryland. The OIG focused this evaluation within the boundaries of the GSS LAN, CPSRMS, ITDSRAM and www.cpsc.gov systems.

Methodology

We conducted this review in accordance with the Quality Standards for Inspection and Evaluation established by the Council of Inspectors General on Integrity and Efficiency's and not the Generally Accepted Government Auditing Standards issued by the Government Accountability Office. The CIGIE standards require that we obtain sufficient data to provide a reasonable basis for reaching conclusions and require that we ensure evidence supporting findings, conclusions and recommendations is sufficient, competent, and relevant, such that a reasonable person would be able to sustain the findings, conclusions, and recommendations.

As part of our evaluation of the CPSC's compliance with FISMA, we assessed the CPSC using the security requirements mandated by FISMA and other Federal information security policies, procedures, standards, and guidelines. Specifically, we:

(1) Used last year's FISMA independent evaluation as a baseline for this year's evaluation;

(2) Reviewed the CPSC's POAM process to ensure that all security weaknesses are identified, tracked, and addressed; and,

(3) Reviewed the processes and status of the CPSC's information security program against the following FISMA reporting metrics: continuous monitoring, configuration management, identity and access management, incident response and reporting, risk management, security training, remote access, contingency planning, and security capital planning.

(4) The statuses of each of these topics were reviewed and discussed with the CPSC's Acting CIO, Director of ITTS, CISO, and relevant members of their staffs. Documentation developed by both CPSC officials and contractor personnel was reviewed. The documentation identified below was considered necessary for the testing of the required FISMA areas:

- ✓ continuous monitoring solution configurations and reports
- ✓ configuration baselines and scan/exception reports
- ✓ user inventory reports
- ✓ incident response reports
- ✓ POAM reports
- ✓ user agreements
- ✓ property reports
- ✓ backup reports
- ✓ employee and contractor rosters
- ✓ MOUs & ISAs
- ✓ planning documents
- ✓ vulnerability reports and system scanning results
- ✓ change control forms
- ✓ risk documentation
- ✓ security training content/reports
- ✓ system configurations
- ✓ contingency plans
- ✓ system inventories
- ✓ agency templates
- ✓ contracts and Statement Of Works (SOWs)
- ✓ meeting minutes

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.

Please note: That names, IP addresses, and system/remote access protocols were omitted from this report due the sensitive nature of this information.

APPENDIX C: CRITERIA

Department Of Homeland Security (DHS):
2015 IG Federal Information Security Modernization Act metrics
HSPD 12, *Homeland Security Presidential Directive 12*
http://www.us-cert.gov/government-users/reporting-requirements)

Federal Information Processing Standards (FIPS):
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems;*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;
FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;

Office of Management and Budget's (OMB) Memorandums:
OMB Circular A-130, appendix iii, *Security of Federal Automated Information Resources*
OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
OMB M-08-05, *Implementation of Trusted Internet Connections (TIC)*
OMB M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
OMB M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*
OMB M-11-27, *Implementing the Telework Enhancement Act of 2010: Security Guidelines*
OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*
OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
OMB M-15-01 *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*

National Institute of Standards and Technology (NIST) Special Publications (SP):
NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*
NIST SP 800-30 (Revision 1), *Guide for Conducting Risk Assessments*
NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*
NIST SP 800-37 (Revision 1), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*;
NIST SP 800-40 (Revision 3), *Guide to Enterprise Patch Management Technologies*
NIST SP 800-45 (Version 2, Guidelines on Electronic Mail Security
NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
NIST SP 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-60 (Revision 1), *Guide for Mapping Types of Information and Information Systems to Security Categories*
NIST SP 800-61 (Rev 2), *Computer Security Incident Handling Guide*
NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

Other NIST guidance:
http://csrc.nist.gov/groups/STM/cmvp/
http://nvd.gov

Federal Emergency Management Agency Directives
Federal Continuity Directive 1 (FCD1)

Federal Register
5 Code of Federal Regulations (5 C.F.R. 930-301)

APPENDIX D: ACRONYMNS & ABBREVIATIONS

Acronym/Abbreviation	Description
AD	Active Directory
ATO	Authorization to Operate
BIA	Business Impact Analysis
BCP	Business Continuity Plan
CAPEC	Common Attack Pattern Enumeration and Classification
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COOP	Continuity Of Operation Plan
CPSIA	Consumer Product Safety Improvement Act
CPSC	Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
CSIRT	Computer Security Incident Response Team
DCM	Dynamic Case Management
DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
DR Plan	Disaster Recovery Plan
EA	Enterprise Architecture
EXIT	Office Of Information Technology
EXRM	Office of Resource Management
FCD1	Federal Continuity Directive 1
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GISRA	Government Information Security Reform Act
GSS LAN	General Support System Local Area Network
HSPD 12	Homeland Security Presidential Directive 12
IEEE	Institute of Electrical and Electronics Engineers

ISA	Interconnect Security Agreement
ISCM	Information System Continuous Monitoring
ISCP	Information System Contingency Plan
ISSO	Information Systems Security Officer
ITTS	Information Technology and Technical Services
ITDSRAM	International Trade Data System/Risk Automation Methodology System
MSS Settings	Microsoft Solutions for Security Settings
MOU	Memo Of Understanding
MTIPS	Managed Trusted Internet Protocol Services
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
POAM	Plan Of Actions and Milestones
RPO	Recovery Point Objective
SANS	Escal Institute of Advanced Technologies
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TIC	Trusted Internet Connection
TT&E	Training, Testing and Exercises
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

APPENDIX E: MANAGEMENT RESPONSE

From: Burrows, Daniel
Sent: Thursday, November 12, 2015 1:00 PM
To: Manley, Patrick
Subject: RE: FY 2015 FISMA Audit Management Responses

Hi Pat,

For the following findings where you stated that "Not enough time allotted to research and provide a meaningful response." How many more days do you need for a response?

ISS.14 Management has not formally applied USGCB and accepted the associated variances -- 2.1.4, 2.1.5, and 2.1.8
ISS 23 RPOs not met – 9.1.11
ISS.42 User access SOPs are missing or do not contain all requisite information - 3.1.1
ISS.43 Management has not fully implemented the General Access Control Policy - 3.1.1
ISS.35 Dual accounts for Administrator - 3.1.5
ISS.36 Principle of Least Access - SOD - GSS LAN 3.1.5
ISS.44 Principle of Least Access - SOD - cpsc.gov - 3.1.5
ISS.52 Information system access is not always disabled immediately upon a users separation-3.1.7
ISS 24 Remote Access Policies and Procedures not implemented - 8 1 1
ISS 27 Remote Access Policies and Procedures inadequate and out-of date - 8 1 1
ISS 25 Missing laptops-Blackberries were not reported to ISSO-CSIRT upon discovery - 8 1 8
ISS.38 Risk not addressed from an organizational perspective - 5.1.1-5.1.3 & 5.1.10
ISS.40 SSPs do not include all required information_5.1.6_5.1.7
ISS.39 Management is not actively engaged in Risk Management - 5.1.12

Thank you,
Dan

Dentel, Christopher

From:	Manley, Patrick
Sent:	Monday, November 30, 2015 11:04 AM
To:	Murphy, Leeann
Cc:	Dentel, Christopher; Burrows, Daniel
Subject:	RE: Management Response to FISMA

Leeann,

I was out of the office last week (just got back today) and haven't seen the final report. I will look at it today but I was under the impression that the period for providing responses had already passed. We provided responses for the findings that were originally provided to us—within the timeframes that we were given. We were not prepared (or anticipating) to provide any additional responses—beyond what was already provided. My assumption was that the final report would only be a narrative of the findings that we were already given. Is this not correct?

Patrick Manley, CISSP
CHIEF INFORMATION SECURITY OFFICER
CONSUMER PRODUCT SAFETY COMMISSION
(O) 301-504-7734
(C) 240-393-1073

From: Murphy, Leeann
Sent: Monday, November 30, 2015 10:53 AM
To: Manley, Patrick
Cc: Dentel, Christopher; Burrows, Daniel
Subject: Management Response to FISMA

Good Morning, Pat -

I am following up on the FY 2015 FISMA Report that Dan provided to you. We would like to know, if management will be providing any additional edits/comments/responses to the report? If so, please provide them today.

By COB today, the OIG will move forward with finalizing and issuing the report.

If you have any questions or concerns regarding the report, please contract Dan or I.

Thanks,
LeeAnn A. Murphy
Deputy Inspector General - Audits
Office of Inspector General
U.S. Consumer Product Safety Commission
4330 East-West Highway, Office 702-G
Bethesda, Maryland 20814
☎: *(301)-504-7685*
📱: *(202)-329-3373*
📠: *(978)-244-8635*
✉: *Lmurphy@cpsc.gov*