U.S. CONSUMER PRODUCT SAFTEY COMMISSION

OFFICE OF INSPECTOR GENERAL

FY 2016 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW REPORT

Issued: 12/14/2016

This report conveys the results of the OIG's review of the CPSC's compliance with the Federal Information Security Modernization Act.

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 14, 2016

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 Modernization Act (FISMA) Evaluation

The Federal Information Security Modernization 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).

The evaluation was performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE), Quality Standards for Inspection and Evaluation (QSIE). 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 35 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
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 Modernization Act (FISMA). In evaluating the CPSC's progress in implementing its agency-wide information security program, we specifically assessed 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 the CPSC continues to make progress in implementing the FISMA requirements. The accomplishments in implementing FISMA requirements include:

- ✓ The maintenance of the General Support System (GSS LAN), Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDSRAM) application, and the CPSC public website (cpsc.gov) security accreditation.
- ✓ The implementation of a new cloud-based website solution to replace cpsc.gov and the completion of this solution's security accreditation.
- ✓ The Computer 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 taken proactive steps in addressing its existing security weaknesses by adding cybersecurity resources to the agency staff and hiring a Chief Information Officer (CIO) with a strong cybersecurity background. In addition, the CPSC has improved its policies and procedures, implemented new cybersecurity solutions, and is actively working toward standardizing its risk documentation. These efforts demonstrate management's commitment to improving the agency's security profile. However, the OIG identified several security weaknesses in the CPSC's management, operational, and technical controls policies, procedures, and practices that remain. 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 reports 35 findings in this year's FISMA review. The information technology (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
  - An incomplete hardware/software inventory;
  - Incomplete documentation and implementation of baseline security configurations and assessments of the risks associated with acceptable deviations from these baselines; and

- Agency systems were not patched in a timely manner.

✓ Identity and Access Management
- Implementation the Principle of Least Privilege and proper segregation of duties for the GSS LAN has not occurred;
- Multifactor authentication is not systematically enforced;
- Remote access controls are inadequate; and
- Inadequate control over the utilization of shared user accounts.

✓ Incident Response
- The OIG assessed the CPSC's Incident Response program using the Incident Response Maturity Model. The maturity model consists of five levels, our assessment found that the CPSC has achieved level one and has made progress toward achieving level two.

✓ Risk Management
- Implementation of the National Institute of Technology and Standards (NIST) Special Publication (SP) 800-37 is incomplete;
- Not all agency information systems have formal authorization to operate;
- The inventory of agency systems is incomplete; and
- The Plan of Actions and Milestones (POAMs) do not include all required information.

✓ Security Training
- Inadequate identification of, and provision of role-based training to, resources with significant security and privacy responsibilities,; and
- The CPSC security and privacy training program does not contain adequate metrics to measure program effectiveness.

✓ Contingency Planning
- Lack of a Business Impact Assessment (BIA), a Business Continuity Plan (BCP), a Disaster Recovery (DR) Plan, and a Continuity of Operations Plan (COOP); and
- The current Information System Contingency Plans (ISCPs) were neither authorized by management nor tested.

✓ Contractor Systems
- Interconnection Security Agreements (ISAs) were not established and/or updated for all relevant CPSC third party systems.
- IT contracts for goods and services did not include all requisite information, including the recommendations for cloud-based services described in the Chief Acquisition Officers (CAO) Council Best Practices Guide for Acquiring IT as a Service for cloud-based services.

- ✓ 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 achieved level two.

MANAGEMENT'S RESPONSE

Management is solely responsible for the Management Response. The factual assertions made in the responses from management were not audited or otherwise formally verified by the OIG.

Management generally concurred with our findings and recommendations. Management did not concur with our finding regarding their inventory of major applications and their software inventory. Management's nonconcurrence and our response are found on pages 6 and 7 of this report.

RESULTS AND FINDINGS
Risk Management

FISMA requires security authorizations for all systems operated by Federal agencies. Further, it requires agency management to assess and monitor security controls on a continuous basis using a risk-based approach based on Federal Information Processing Standards (FIPS), OMB, and NIST guidance. Once an agency performs the initial authorization of a system, management should use the results of on-going security assessments and monitoring tasks, as a basis for the system to continue Authorization to Operate (ATO). This requires agencies to develop a process and establish an infrastructure to frame, assess, respond to, and monitor risk. In addition, 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 the documentation requirements for each known security weakness.

Progress:
The CPSC has begun to update the System Security Plan (SSP) control implementation catalogs for authorized systems, in order to align them with the latest revision of the NIST SP 800-53 guidance, released in April of 2013. According to management and independent assessors, the agency has completed approximately 2/3^{rds} of updates and estimates completion in Fiscal Year (FY) 2017. In addition, the CPSC updated the Security Assessment Reports (SARs) and POAMs associated with accredited systems in FY 2016 and completed the security authorization for new agency website. Furthermore, the IT security team issues monthly security status reports to Senior IT management to provide 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, the agency has not: ✓ Created an Organization-wide Risk Management Strategy to ensure risks to the mission and organization are considered. ✓ Established a Risk Executive (function) or established a comprehensive governance structure to manage risk. ✓ Defined an adequate methodology that may be used to calculate the agency's Organizational Risk Tolerance. ✓ Developed an Enterprise Architecture (EA); therefore, the CPSC has not integrated the EA into the agency's risk management process.	*Management concurs with this finding.* *Management has informal risk management processes in place—such as POAM tracking, user account reviews, and role-based access monitoring. While a formal framework is not currently in place, governance processes consider organizational risk factors. CPSC has put in place a contract which will result in the development of a formal organizational risk management plan.* *The Office of Information Technology (EXIT) hired an Enterprise Architect in 2016.*

✓ Integrated organizational/mission perspectives into the system level risk assessments.	
The CPSC's inventory of major systems is incomplete. The OIG's primary concern is that there are still unidentified systems residing on the CPSC network and that existing applications are not classified as major or minor, appropriately. OMB Circular A-130 defines a major system as one that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. However, the CPSC has defined several of these systems as minor systems even though these systems perform a significant role in agency programs, finances, and property administration. In addition, the agency has not developed a comprehensive software inventory, nor has it authorized any agency system outside of the five defined, as major. The current inventory is a partial listing of CSPC systems, which is informal and incomplete. Further, not all of the systems listed were authorized, as required by OMB M-10-15. Also, the CPSC has not categorized or adequately justified the categorization of each of these systems and has not selected, implemented, or assessed all of the requisite security controls employed by all of the systems listed in the inventory.	*Management does not concur with this finding.* *Management provided a formal Major Applications inventory to the auditor which identified all of the applications that Management formally classified as "major applications." The auditor disagreed with Management's inventory—specifically citing the lack of major applications related to finance and inventory systems. However, the systems that the auditor believes should be classified as "major" are either third-party applications (managed by another agency) or applications that inherit the majority of their controls from the agency's general support system (GSS LAN)—which is classified as a major application. Management believes that its application classification process is in accordance with guidance provided by NIST SP 800-18 and that its systems inventory is complete. In FY 2016 Management performed security assessments and classifications of the agency's minor applications—which are contained within the GSS LAN security boundary.* *Management reviewed OMB M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, as well as NIST 800-18 rev 1 and believes that the agency's major systems and designations authorizations are in accordance with relevant guidance.* ***OIG Response:*** *After reviewing the arguments raised in the Management Response, the OIG stands by its assessment of the agency's inventory of major systems.*

	According to A-130, all systems that play a significant role in the administration of agency programs, finances, property, or other resources are considered major systems. Management has not classified systems responsible for these tasks as "major." *Management is given great latitude when determining the boundary of a system. However, this latitude is not infinite and must be determined in accordance with Federal guidance, and the methodologies/processes employed to make these determinations should be established by agency policies and procedures.* *Management has not developed and policies and procedures that document how it defines system boundaries or how it determines if a system is major or minor. As a result, it is unclear how the determination of whether any individual system is considered major or minor was made at the CPSC. In addition, when defining a system boundary management must identify/document all components of the system; and the CPSC has not done this with the GSS LAN. Management has not formally documented what applications/subsystems reside within the GSS LAN's system boundary. The informal inventory of agency applications supported by the GSS LAN that was provided to the OIG by management was incomplete.* *Finally, the Management Response failed to address the portion of the finding relating to the CPSC's failure to develop a comprehensive software inventory.*
The CPSC's existing SSPs do not include all required information: ✓ The SSPs for accredited systems do not reflect all the changes in the April 2013 revision of NIST SP 800-53. ✓ Neither all the security controls for a moderate impact	*Management concurs with this finding.* *Current practices are substantially effective. In FY 2016 Management completed assessments of the final 1/3 of security controls that had not been assessed at the NIST SP 800-53 rev 4*

system nor documentation of the justification for not implementing these controls, as required by NIST SP 800-53, were accomplished by the agency. The GSS LAN included neither a description of the agency systems within the security boundary of the GSS LAN in the GSS LAN SSP nor all the data types described in all of the Major Applications' SSPs.	*level. The independent assessment was completed after the FISMA auditor's evaluation. All security control documentation has been updated accordingly. Management believes that this portion of the finding has been appropriately addressed.* *In FY 2016 Management performed security assessments and classifications of the agency's minor applications. In FY 2017 Management will develop a formal system boundary document from this information and include in the GSS LAN SSP.* *In FY 2017 Management will update the GSS LAN SSP to include all of the data types described in all of the major application SSPs.*
The CPSC did not adequately perform the Information System categorization for all agency systems. We identified that the CPSC: ✓ Could not provide evidence that the "special factors" documented in NIST SP 800-60 Volume II, Appendices C & D were considered when determining the final impact of each of the identified NIST SP 800-60, volume II data types. ✓ Did not include all of the data types described in all of the Major Applications SSPs in the GSS LAN SSP, even though the GSS LAN provides common controls to those systems. ✓ Has not categorized all minor applications.	*Management concurs with this finding.* *Current practices are substantially effective. Management reviewed NIST SP 800-60 Volume II, Appendices C & D, and determined that there are no "special factors" that would result in the elevation of any agency system above its current classification. Management will add this notation to updated security plans.* *In FY 2017 Management will update the GSS LAN SSP to include all of the data types described in all of the major application SSPs.* *Management provided the auditor with security assessments performed on all agency minor applications—which included categorization information.* *Documentation updates are needed to clarify interpretations.*

The OIG reviewed the CPSC's POAMs and found that the agency had not documented all information required by OMB M-04-25 nor was the required information for all security weaknesses documented consistently. These deficiencies included: ✓ Missing completion dates ✓ Unique Project Identifiers that ties it to its associated budget documentation (ex. Exhibit 53/300s/Spend Plans) ✓ Inaccurate references to the organizations responsible for remediating the security weaknesses	*Management concurs with this finding.* *Management believes that its POAM management process is substantially effective but acknowledges some missing non-critical data fields for some POAM items. Management has significantly increased attention to POAM completion which resulted in a —47 percent reduction in FY 2016 and intends to maintain this level of attention to continue improvements in POAM performance. In FY 2016, Management began a process of migrating POAMs into a web-based, security governance system – Cyber Security Assessment and Management (CSAM).*
The CPSC has not adequately developed risk management documentation for the Drupal implementation to include: ✓ An adequately documented risk assessment for the Drupal implementation. ✓ A properly developed and documented POAMs for the Drupal implementation. ✓ Further the CPSC has not: ✓ Developed/documented POAMs for all of the known security weaknesses associated with the Drupal implementation. The Drupal SAR indicates that 285 (84%) of the 339 documented security controls are not implemented. However, the agency has only developed and documented 37 POAMs, of which only 57 (20%) of 285 documented security weaknesses are addressed. ✓ Documented milestones, milestone dates or changes to milestones/milestone dates for the documented security weaknesses associated with the Drupal implementation.	*Management concurs with this finding.* *Management believes there is some misinterpretation of the Drupal SAR. Drupal has 58 documented system-specific security controls that are not implemented as opposed to the reported 285. These are appropriately recorded in the agency's security governance system. Additional controls specified in the SAR are classified either as "Not Applicable" or are common controls.* *Drupal's security controls were assessed and POAMs created at the end of FY 2016. Not all milestones had been determined at the time of the audit. The Drupal system owner is working with IT Security staff to document appropriate milestone dates. The risk assessment documentation will be reviewed in FY 2017*

Recommendations:

We recommend that management:

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

2. Develop a comprehensive EA and integrate the EA into the risk management process.

3. Document and certify a complete systems inventory that includes all CPSC systems (both major and minor systems), and include a description of each system in this systems inventory.

4. Review and certify the inventory of all systems annually, and in the event of a major change. Ultimately, this inventory should tie to the agency's EA. The systems inventory (or supporting risk assessments) should include:
   - ✓ the interfaces with all other systems/networks,
   - ✓ the system criticality (based on a current BIA),
   - ✓ the security categorization (based on FIPS 199),
   - ✓ if the system is considered a major system or a minor system and adequate rational for the designation.
   - ✓ the hardware utilized by the system,
   - ✓ the databases utilized by the system,
   - ✓ the ATO status of each system, and
   - ✓ the name of the system owner.

5. Categorize each of the agency's systems (including all of the CPSC's minor applications), and select, implement, and assess the security controls employed by each of these systems. The CPSC should report this information in the existing risk documentation (ex. SSP/SAR/POAM), where appropriate.

6. Formally authorize the operation of each agency system, including the agency's minor systems, once the risk associated with those systems is known and accepted. This can be included in the assessment of a larger system, if a risk assessment was performed/documented and the minor applications security controls were implemented.

7. Create/update security plans for all major agency systems and include all NIST SP 800-53, Revision 4 selected controls in these plans.

8. Update existing security plans to describe how all of the selected security controls are implemented.

9. Update the existing security plans, where applicable, to include a description of all agency systems and data types, and include a description of how the controls selected for each of the minor applications are implemented.

10. Perform and document a formal assessment to categorize all agency systems based on the NIST SP 800-60 guidance. This should include:
    - ✓ Identifying all relevant data types for all agency systems and documenting these data types in all relevant agency SSPs or categorization documents.
    - ✓ Performing an assessment to determine the final impact of each data type on the agency mission based on the following process:
    - ✓ Identifying the provisional impacts of each of the documented data types for each system.
    - ✓ Adjusting the data type impact based on the "special factors" described in NIST SP 800-60, Volume II and documenting this information in the SSP or related categorization document. This task should be performed by the relevant mission owners.
    - ✓ Determining the data type final impact. This should be determined based on the coordinated efforts of the mission owners and EXIT and documented in the SSP or related categorization document.

11. Document all of the OMB M 04-25 required information for all security weaknesses tracked in the agency POAMs. The POAMs should include:
    - ✓ Unique Investment Identifiers/Unique Project Identifiers (UIIs/UPIs) to allow agency officials to trace the security weakness to the budget documentation.
    - ✓ Completion dates for the remediation of all security weaknesses, where practical.
    - ✓ The organization responsible for remediating the security weaknesses.

12. Document a comprehensive risk assessment for the Drupal implementation in accordance with NIST guidance,

13. Develop/document POAMs for all of the known security weaknesses associated with the Drupal implementation in accordance with OMB M-04-25.

Continuous Monitoring

OMB Memorandums and NIST Special Publications provide guidance, in an effort to ensure agencies develop processes for real time risk management and monitor their security posture on a continuous basis. In addition, the Council of Inspector Generals on Integrity and Efficiency (CIGIE) released an Information System Continuous Monitoring (ISCM) maturity model in FY 15. 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 (unchanged for FY 16), we assessed the CPSC's ISCM program to determine the agency's current ISCM maturity level. Based on our review, we determined that the CPSC has achieved level two.

Progress:
The CPSC has reviewed and updated the ISCM Policy, Strategy, and Risk Assessment documents in FY 2016 to facilitate compliance with FISMA requirements. The ISCM Strategy included the list of security controls employed, testing frequencies, and schedules. The ISCM Strategy also included the list of security metrics monitored, their assessment, and reporting frequencies. Senior IT management received periodic ISCM metric status reports, reports on the results of ongoing assessments, and the remediation efforts to assist with risk management. This process will continue to improve with the implementation of new monitoring tools to optimize the existing tool set. In FY 2017, the CPSC plans to complete the implementation of the ISCM program, as part of the phased approach described in OMB M-14-03.

Issues to Be Addressed:	**Management Response:**
The CPSC 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: ✓ the CPSC 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 it was not included in the Roles and Responsibilities section of the ISCM Policy. Moreover, the CPSC has not established a Risk Executive (function) to perform the tasks outlined in the ISCM Plan.	*Management concurs with this finding.* *Current practices are substantially effective. Management believes that all the roles/responsibilities required to successfully implement and manage the agency's ISCM program have been appropriately assigned and stakeholders were advised of their responsibilities (scanning, assessment coordination, etc.).* *Although currently the "Risk Executive" role at the agency has not been formalized, the functions ascribed to this role are performed at various levels within the agency.*

	Documentation updates are needed to clarify interpretations.
The CPSC did not perform a knowledge, skills and abilities "Gap Analysis" to identify, prioritize, and remediate the capabilities necessary to establish and support the agency's ISCM strategy. The ISCM Gap Analysis included in the ISCM Plan did not include a description of the knowledge, skills, and abilities required to implement the agency's ISCM strategy, a description of the gaps in those capabilities, or the solutions involved with implementing these deficiencies.	*Management concurs with this finding.* *Current practices are substantially effective. Management did not perform a formal "gap analysis;" however personnel assigned significant ISCM responsibilities receive appropriate training and development through formal classroom training, seminars, and mentoring.* *Documentation updates are needed to clarify interpretations.*
The ISCM plan 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, the CPSC 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 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 the CPSC considers reauthorizing a major agency system, as is suggested in the agency's ISCM risk tolerance statement.	*Management concurs with this finding.* *Current practices are substantially effective. Management will review the ISCM Plan's system reauthorization requirement to ensure that reauthorization decisions are more closely aligned with specific security event metrics/triggers (i.e., PII breach, insider threat sabotage, etc.).* *Management believes that its current ISCM process, which provides that reauthorization decisions be based on the occurrence of specific issues or events, is compliant with NIST Supplemental Guidance on Ongoing Authorization. This guidance stipulates that, "under OA, reauthorization is typically an event-driven action initiated by the AO or directed by the Risk Executive (function) in response to an event."*
The CPSC has not defined and documented a process to capture the lessons learned to improve the effectiveness of the ISCM program.	*Management concurs with this finding.* *Current practices are substantially effective. Management has not documented a formal "lessons learned" process; however, Management reviews the ISCM program when significant events*

	occurs to identify root causes and recommendations for program effectiveness.
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 ✓ Malware ✓ Information management/Data Loss Prevention ✓ Software assurance	*Management concurs with this finding.* *Current practices are substantially effective. Management currently has a robust malware scanning/detection capability in place—malware-related security incidents were reduced by 80 percent between FY 2015 and FY 2016. Management has allocated resources and expects to implement a data loss prevention capability in FY 2017. Management currently has manual processes in place to manage software licenses and expects this process to become fully automated with the implementation of the DHS CDM program. Technologies related to software assurance will also be addressed by CDM.* *Documentation updates and additional automated tools are needed to fully address this finding*

Recommendations:

We recommend that management:

1. 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. Perform a Gap Analysis to identify the missing knowledge, skills, and abilities required to implement the ISCM program.

3. Develop a remediation plan for each of the shortfalls noted in the ISCM Gap Analysis.

4. Implement the remediation plan, noted above.

5. Periodically reassess the ISCM program for knowledge, skills, and abilities gaps as the ISCM process matures.

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

7. Integrate the organizational risk tolerance described in the Organization-Wide Risk Management Strategy into the agency's ISCM strategy.

8. Formally define and implement a process that facilitates consistently capturing and sharing the lessons learned related to the effectiveness of ISCM processes and activities.

9. Identify, fully define, and develop a plan for implementing the ISCM technologies it expects to utilize in the following automation areas:
   - ✓ License management
   - ✓ Malware
   - ✓ Information management
   - ✓ Software assurance

Contingency Planning

FISMA requires that agencies develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. The Federal Emergency Management Agency (FEMA), NIST, and the National Archive and Records Administration (NARA) provide additional guidance for Federal agencies contingency planning efforts.

Progress:
The CPSC has not made any additional progress in this process since the last OIG review. However, the agency hired a contractor to perform and document a BIA; as well as, draft and test ISCPs for five systems (GSS LAN, CPSRMS, DCM, ITDSRAM, and cpsc.gov).

Issues to Be Addressed:	**Management Response:**
The CPSC has not developed and implemented policies and procedures that: ✓ enumerate the test, training, and exercise (TT&E)	*Management concurs with this finding.* *Management has put in place a contract which will result in the*

program requirements defined in Federal Continuity Directive 1(FCD1); ✓ codify all of the FDC1, Appendix A required information; ✓ require the development and maintenance of necessary contingency planning documentation (ex. BIAs, DR Plans, BCPs, and COOPs); ✓ require that the ISCPs be used in the coordination and development of organization-wide plans such as the COOP, DR Plans and BCPs; ✓ ensure that supply chain threats are considered; ✓ require an assessment of the resource requirements for the contingency planning process, as recommended by NIST SP 800-34; and ✓ adequately support NARA data retention requirements.	*development of a formal Business Impact Assessment (BIA), major application contingency plans, and major application contingency test plans.*
The existing CPSC Contingency Planning Policy is not implemented nor have several critical contingency planning documents necessary to facilitate its implementation been developed, as the CPSC 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 all of the agency's existing ISCPs in FY 2016; and ✓ established an Alternative Processing Site.	*Management concurs with this finding.* *Management has put in place a contract which will result in the development of a formal Business Impact Assessment (BIA), major application contingency plans, and major application contingency test plans.* *Management has not formally established an Alternate Processing Site. Management is anticipating clarification of the extent of this need to be an outcome of the BIA and contingency planning work planned for FY 2017. Although a formal plan has not been established EXIT has implemented robust tape backup processes to ensure that critical agency data is appropriately backed up and stored offsite—in secure tape storage facilities. Management also employs "data snapshots"—which automatically replicate critical agency data, at least once a day, to the data center located offsite at the National Product Testing and Evaluation Center located in Rockville, MD. Some of the currently presumed most critical functions have partial fail over*

	capability to the secondary data processing site.
Data retention strategies employed by the CPSC do not meet the retention requirements described in the NARA General Schedule 3.2. Specifically, the agency does not retain: ✓ Public Key Infrastructure related information for at least seven years and six months; and ✓ computer security incident handling, reporting and follow-up records for at least three years.	*Management concurs with this finding.* *Management will review its backup strategy and ensure that PKI and incident handling data are backed up and maintained in accordance with the NARA General Schedule.*
The CPSC does not employ backup strategies to meet the Recovery Point Objectives (RPOs) documented in the ISCP. Specifically, the CPSC cannot achieve the documented RPOs with the agency's current backup schedules.	*Management concurs with this finding.* *The referenced recovery point objectives will be updated as part of the work associated with the contract to develop a formal BIA and system contingency plans.*

Recommendations:

We recommend that management:

1. Develop and implement an FCD1 compliant TT&E program.

2. Update the contingency planning policy and develop procedures to:
   - ✓ require the development and maintenance of necessary contingency planning documentation (ex. BIAs, DR Plans, BCPs, and COOPs);
   - ✓ require that the ISCPs be used in the coordination and development of organization-wide plans such as the COOP, DR Plans and BCPs;
   - ✓ require an assessment of the resource requirements for the Contingency Planning process as required by NIST SP 800-34
   - ✓ ensure that supply chain threats are considered;
   - ✓ enumerate the TT&E program requirements defined in FCD1;
   - ✓ codify all of the FDC1, Appendix A required information; and
   - ✓ codify retention schedules in accordance with the NARA General Record Schedules.

3. Implement the updated contingency planning policies and new contingency planning procedures.

4. Establish, document, test, and approve a DR Plan, BCP, and COOP.

5. Draft After-Action Reports to document the "lessons learned" identified, as part of the COOP, DR, and BCP plan testing.

6. Perform, document, and approve a formal BIA in accordance with NIST SP 800-34.

7. Establish, formalize, test, and approve ISCPs for all critical agency systems in accordance with FEMA guidance.

8. Establish an Alternative Processing Site. This site should contain the equipment and supplies required to recommence operations in time to support the organization-defined period for resumption.

9. Train all relevant resources on the continuity planning responsibilities assigned to them in the policy.

10. Document a NARA compliant retention plan for all relevant agency data in a policy or procedure.

11. Update its retention schedules to meet the retention policies and procedures.

12. Document an RPO for all relevant agency systems.

13. Implement a solution to allow management to meet the RPOs for all relevant systems.

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." These services include those 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 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. These contracts and agreements must include appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation (FAR) clauses, and clauses on protection, detection, and reporting of information; in addition to a description of how information security performance is measured, reported, and monitored. Agencies also must obtain sufficient assurance that the security controls of contractor systems meet FISMA requirements.

Progress:
The CPSC maintains a policy that governs the oversight of contractor systems and has developed an inventory of CPSC's third-party systems. In addition, the agency has established a process to review contracts for the inclusion of standard procurement clauses.

Issues to Be Addressed:	**Management Response:**
The OIG conducted a review over a sample selection of CPSC IT contracts to determine whether the required disclosures are included in each contract/agreement. Through our review, we identified the following FAR clauses and NIST requirements that were not consistently included in the IT contracts/agreements: ✓ FAR 52.224-1, Privacy Act Notification clause; ✓ FAR 52.224-2, Privacy Act clause; ✓ FAR 52.239-1 Privacy or Security Safeguards; ✓ FAR 39.105 Privacy; ✓ FAR 39.101Policy; and ✓ NIST SP 800-53, SA-4 requirements. In addition, the CPSC has not established a process to ensure that all of the recommendations outlined in the *CAO Council Best Practices Guide for Acquiring IT as a Service* are included in the agency contracts for cloud-based services. This resulted in not including the following information in a cloud contract: ✓ enforcement mechanisms in place to ensure SLA requirements are met; ✓ a requirement that Cloud Service Providers route their traffic through a Trusted Internet Connection (TIC); ✓ continuous monitoring programs; ✓ the Cloud Service Provider's liability for data security; ✓ compliance with the CPSC's Computer Security Incident Handling requirements; ✓ Freedom of Information Act processing requirements; and	*Management concurs with this finding.* *Current practices are substantially effective.* *Management provided the requisite security clauses to the agency's Procurement Office to include in future IT contracts.* *Management will meet with Procurement to discuss additional requirements.* *The Best Practices Guide will be reviewed, however, Management believes it is compliant with all federal cloud-based system guidance—all of the agency's current cloud-supported systems are maintained by FedRAMP-approved service providers.*

✓ NARA requirements.	
The CPSC has not developed SOPs to support the Contractor Security Oversight policy. In addition, the Contractor Oversight Policy is missing the following information: ✓ How frequently management is to be provided with and must examine the security review/ATO documentation to ensure contractors remain in compliance with FISMA. ✓ A requirement for management to perform an assessment of the third party interfacing system's user controls. ✓ The process to ensure that appropriate agreements include how information security performance is measured, reported, and monitored on contractor or other entity-operated systems.	*Management concurs with this finding.* *Current practices are substantially effective. Management reviews ISA's annually and requests valid ATO documentation when current contractor system ATOs expire.* *In FY 2016 Management completed assessments of the interfacing security controls for all third-party systems.* *Agency policy stipulates that the agency will utilize the third-party system's current ATO as a validation that security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
The CPSC does not ensure that all connecting third party systems are FISMA compliant, this should be, but is currently not, accomplished by: ✓ ensuring that all contracted, third party systems maintain a current security authorization (i.e. ATO); ✓ ensuring that all FISMA and related policy requirements are implemented and reviewed in accordance with FISMA guidance; ✓ authorizing connections through the use of Interconnection Security Agreements for external information systems; and ✓ performing an annual review of third-party systems.	*Management concurs with this finding.* *Current practices are substantially effective however the agency is subject to cooperation of service providing agencies to approve documentation in a timely manner. Management believes that its internal processes, related to contractor system security agreements, are effective and fully compliant. Management obtained approved ATO's and security agreements for all contractor systems—except for two systems in which the hosting agencies were unresponsive to CPSC requests for updated agreements.*

Recommendations:
We recommend that management: 1. Develop a formal process to ensure that all requisite FAR clauses and security information is included in contracts/agreements moving forward.

2. Establish coordination between the Division of Procurement Services (FMPS), Office of the General Counsel (OGC), and the Office of Information Technology (EXIT) to ensure that all of the recommendations outlined in the CAO's Best Practices for Acquiring IT as a Service are incorporated into agency policies, procedures, practices, and third-party agreements.

3. Update the Contractor Oversight Policies and develop attendant Procedures to include the following:
   - ✓ The frequency that management must be provided with and review the security review/ATO documentation to ensure contractors remain in compliance with FISMA.
   - ✓ A requirement to perform an assessment of user controls.
   - ✓ The process by which the agency ensures that appropriate agreements include descriptions of how information security performance is measured, reported, and monitored for contractor- or other entity-operated systems.

4. Establish and implement processes and procedures to ensure all connecting systems meet FISMA requirements. This includes the active maintenance of a third-party systems inventory.

Configuration Management

According to the Center for Internet Security's (CIS) Critical Security Controls for Effective Cyber defense, agencies are required to actively manage (inventory, track and correct) hardware devices and software executing on the network. This requirement is designed to ensure that unauthorized/unmanaged devices and software are found and prevented from access/installation. This requirement is meant to be accomplished through proper configuration management techniques and processes. The key goal of configuration management is to make assets harder to exploit through better configuration. To this end, FISMA requires agencies to document, implement, and monitor agency compliance with the United States Government Configuration Baseline (USGCB, formally the Federal Desktop Core Configuration) for clients and to document and implement configurations for all other agency systems consistent with the Security Technical Implementation Guidelines (STIGs) found in the Nation Vulnerability Database (NVD). If checklists are unavailable through the USGCB, the NVD, or other checklist repositories, then agencies are required to develop their own. In addition, because of recent cyber-attacks on the Federal Government, OMB/DHS have released memoranda/directives that supplement existing federal guidance requiring the timely patching of agency systems. In order for an agency's configuration management process to be effective, the configuration management process must be complete, accurate and operate in near real-time.

Progress:
The CPSC has not selected, documented, and implemented USGCB/Defense Information Systems Agency/CIS configuration settings to all agency systems, but management has made progress in this endeavor. The agency installed a whitelisting solution (a tool that

limits a user's ability to install unauthorized software to predefined logical locations) on agency clients and plans to implement this solution on its servers in FY 2017. In an effort to improve its ability to restrict unauthorized client software from executing on the network, the CPSC executed a formal review process over local administrator rights on workstations and has a systematic process to remove existing local administrative privileges on a daily basis. Further, the CPSC has continued to improve its automated scanning capabilities. 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:**
The CPSC Configuration Management policies do not include the following information: ✓ how often the CPSC must scan the network for unauthorized hardware/software; ✓ what actions the CPSC must take to remove the unauthorized hardware/software from the network; and ✓ how quickly configuration setting deviations must be remediated or the associated risk accepted.	*Management concurs with this finding.* *Current practices are substantially effective due to mitigating controls. Management has not implemented an automated tool to scan the network for unauthorized hardware/software; however, Management has implemented several compensating controls. In FY 2016, Management implemented an application whitelisting tool that blocks the execution of unauthorized software on agency computers. The agency employs device management tools that block access to unauthorized mobile devices on agency computers. The agency also employs certificate-based authentication to both its wireless LAN and remote connectivity (VPN) systems.*
The Configuration Management Policy is not fully implemented, as it has not: ✓ developed SOPs or a Configuration Management Plan to support the Configuration Management Policy; ✓ developed, documented, and maintained under configuration control baseline configurations for all system components; ✓ formally reviewed and updated existing baseline configurations annually; ✓ identified and documented the types of changes to the	*Management concurs with this finding.* *Management has put in place a contract to develop configuration management plans, baseline configurations, and a component inventory for all of the agency's major applications.*

information system that are configuration-controlled; ✓ established and documented configuration settings for all information technology products employed within the information system using benchmarks or STIGs; ✓ identified, documented, and approved deviations from the agreed upon configuration settings; ✓ reviewed all proposed configuration-controlled changes to the information system and approved or disapproved such changes with explicit consideration for security impact analyses; ✓ developed and documented an inventory of current information system components ; and ✓ employed automated mechanisms to actively detect hardware devices and software on the network.	
The CPSC has not established and implemented a patch management program that supports the timely implementation of client, server, database, and third party patches. ✓ Policies and procedures governing the patch management process do not require critical patches to be applied to agency systems within 30 days in accordance with OMB M 16-04 or describe: o the process by which the CPSC tests patches prior to implementing them into production, o the process by which the CPSC integrates the patch management process into the configuration management process, and o [redacted]; ✓ The steps taken to test patches are not consistently documented change control forms; ✓ Unsupported versions of databases, operating systems,	*Management concurs with this finding.*

and third-party applications are in use; and ✓ [redacted] are not scanned for patch compliance as required by the Risk Assessment Procedure.	

Recommendations:

We recommend that management:

1. Update the Configuration Management policies, and develop and implement SOPs to standardize the implementation of the Configuration Management process. The Configuration Management policies/SOPs should include the following information:
   - ✓ how often the CPSC must scan the network for unauthorized hardware/software;
   - ✓ what actions the CSPC must take to remove the unauthorized hardware/software from the network; and
   - ✓ how quickly configuration setting deviations must be remediated or the associated risk accepted;
   - ✓ references to other relevant policies and procedures.

2. Develop, document, and implement a configuration management plan for agency information systems.

3. Develop, document, and maintain under configuration control baseline configurations for all system components.

4. Formally review and update existing baseline configurations annually.

5. Identify and document the types of changes to the information system that are configuration-controlled.

6. Establish and document configuration settings for all information technology products employed within the information system using benchmarks or STIGs agreed upon by the System Owner and Information System Security Officer.

7. Identify, document, and approve deviations from the agreed upon configuration settings.

8. Review all proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.

9. Develop and maintain a comprehensive inventory of software and hardware.

10. Employ automated mechanisms to actively detect hardware devices and software on the network.

11. Update the Risk Assessment policies/procedures to require the patching of critical agency systems within 30 days in accordance with OMB M 16-04 and to describe:
    - ✓ the process by which the CPSC tests patches prior to implementing them into production;
    - ✓ the process by which the CPSC integrates the patch management process into the configuration management process; and
    - ✓ the frequency that the [redacted] must be patched.

12. Implement client, server, database and third-party 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.

13. Test all client, server, database, and third-party patches in a test environment prior to deploying the patch to the full production domain and document the steps taken to test patches in the change control forms.

14. Add a separate query to the change management database to allow users to search on server, database, and third-party patches.

15. Upgrade to a supported versions of the existing Operating Systems, databases, and third-party applications, or migrate to another supported version of these systems.

16. Scan [redacted] for patch compliance.

Incident Response and Reporting

NIST requires the establishment of incident detection, handling, and analysis policies and procedures. Thus, agencies are required to notify the United States Computer Readiness Team (US-CERT) of security incidents in accordance with the US-CERT Concept of Operations requirements. In FY 2016, CIGIE released an Incident Response (IR) maturity model as part of the annual FISMA metrics. The IR maturity model function in the same way and serves the same purpose as the previously described ISCM maturity model. Using this new model, we assessed the CPSC's IR program to determine the agency's current maturity level. We determined that the CPSC has achieved level one in each of the domains (people, processes, and technology) and has made significant progress in the effort to achieve level two. The findings and recommendations reported here are necessary for management to achieve level two.

Progress:
The CPSC has established a formal CSIRT; documented policies, procedures and strategies; and implemented several automated solutions to support the Incident Response program. [redacted] Although the CPSC has not completed all of the steps outlined in the FISMA maturity model to reach maturity level two, management has taken a proactive approach in identifying, resolving, and reporting security incidents in 2016. In addition, the CPSC's CSIRT has gained experience and improved the existing incident response solutions over the last year to identify, remediate, and report security incidents, while becoming more efficient and effective at detecting, resolving, and reporting security incidents. [redacted]

Issues to Be Addressed:	**Management Response:**
The IR Policy, Plan and Procedures do not define the following: ✓ CSIRT levels of authority; ✓ how Incident Response will be integrated into the Organizational Risk Management; ✓ how Incident Response will be integrated into the Contingency Planning process; ✓ training requirements for Help Desk Specialists, Network Engineering Specialists, Desktop Support Specialists, and Systems Development Specialists based on their IR responsibilities; ✓ a process for notifying congress in the event of a "Major Incident" or document the process for notifying affected individuals in the event of a data breach; ✓ how management collaborates with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents; ✓ the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident	*Management concurs with this finding.* *Current practices are substantially effective.* *Management will update the IR Plan to add missing information.* *Plans to implement data loss prevention systems, file integrity scanners, data flow baselines are not normally included in IR plans. Management began implementation of an agency-wide data loss prevention capability and expects to complete in FY 2017. Management will review requirements for file integrity scanning and data flow diagrams for agency systems.* *Management will disseminate the IR Plan to all appropriate personnel.* *Although not formally documented in FY 2016 EXIT notified DHS and U.S. CERT as required. Additionally EXIT participates in regular briefings with U.S. CERT and coordinates on any non-*

response program, perform trend analysis, achieve, situational awareness, and control ongoing risk; ✓ a plan to implement a data loss prevention solution; ✓ a plan to implement a tool to assess file integrity; and ✓ a plan to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. In addition, The IR Policy and Plan was not disseminated to all users with the CSIRT supporting roles documented in the respective policy/plans.	*standard incident response approaches.*
The CPSC has not performed an assessment of the skills, knowledge, and resources necessary to implement an effective incident response program and developed remediation plans for addressing the gaps identified.	*Management concurs with this finding.* *Current practices are substantially.* *Management did not perform a formal "skills assessment" for personnel with incident response responsibilities; however, personnel with significant IR roles receive appropriate training and development through formal classroom training, seminars, and mentoring.* *Documentation updates are needed to clarify interpretations*

Recommendation:
We recommend that management: 1. Update the IR Policy, Plan and Procedures to define the following: ✓ CSIRT levels of authority; ✓ how Incident Response will be integrated into the Organizational Risk Management; ✓ how Incident Response will be integrated into the Contingency Planning process; ✓ training requirements for Help Desk Specialists, Network Engineering Specialists, Desktop Support Specialists, and Systems Development Specialists based on their IR responsibilities;

- ✓ a process for notifying congress in the event of a "Major Incident" or document the process for notifying affected individuals in the event of a data breach;
- ✓ how management collaborates with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents;
- ✓ the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve, situational awareness, and control ongoing risk based on the process outlined in NIST SP 800-55;
- ✓ a plan to implement a data loss prevention solution;
- ✓ a plan to implement a tool to assess file integrity; and
- ✓ a plan to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.

2. Disseminate the IR Policy/Plan to all users with CSIRT supporting roles documented in the respective policy/plans.

3. Perform a Gap Analysis to identify the missing skills, knowledge, and resources required to implement the IR program.

4. Develop a remediation plan for each of the shortfalls noted in the IR Gap Analysis.

5. Implement the above referenced remediation plan.

6. Periodically reassess the IR program for skills, knowledge, and resource gaps as the IR process matures.

Security Training

NIST and the Code of Federal Regulations (CFR) require the CPSC to provide Security Awareness Training and role-based security trainings to all employees/contractors who have significant information system security responsibilities. In addition, NIST and OMB require agencies to provide privacy awareness and role-based privacy training for personnel with significant privacy responsibilities.

Progress:

The CPSC obtained security awareness and privacy awareness trainings from the Department of the Interior and role-based security training courses from the Department of Veterans Affairs. The agency provided security and privacy awareness training to CPSC personnel in FY 2016. In addition, the agency provided role-based security training to the Office of Information Technology Services (EXIT) personnel that management identified as having significant security responsibilities in an effort to comply with 5 CFR

930.301. The agency is planning on customizing the security awareness and role-based security training in FY 2017 to reflect the CPSC's policies, procedures, processes.

Issues to Be Addressed:	**Management Response:**
The Security Training policies and procedures do not require role-based training for non-IT staff, including those explicitly outlined in 5 C.F.R 930.301. Instead, management has decided to "tailor-out" all users with significant security responsibilities that are not EXIT personnel. In addition, the policies and procedures do not require management to provide role-based training prior to authorizing access to the information system or permitting the user to perform assigned duties.	*Management concurs with this finding.* *Current practices are substantially effective.* *Management will update the EXIT AT policy to add this requirement for FY 2017.*
Personnel who require role-based training did not receive such training in 2016, as follows: ✓ 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. ✓ The role-based security provided did not reflect CPSC specific processes, policies, and procedures.	*Management concurs with this finding.* *Current practices are substantially effective. 100% of users with network access completed mandatory security and privacy training.* *Management, in accordance with agency policy, provides role-based security training for those employees having significant security responsibilities, at least annually. Employees whose job responsibilities include IT security, system administration, database administration, network architecture, application development, website administration, data backup/recovery, email administration, or firewall administration are considered to have significant security responsibilities and receive the appropriate role-based training.* *EXIT will evaluate additional roles to determine potential gaps and clarify expectations.*

Management has not established a policy or procedure that requires management to provide users with "significant" privacy responsibilities specialized privacy training. Management has not identified all users with significant privacy responsibilities and does not provide specialized privacy training to these users.	*Management concurs with this finding.* *In accordance with direction from OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy, the designation of Senior Agency Official for Privacy was reviewed and elevated to the Chief Information Officer, Assistant Executive Director of the Office of Information and Technology Services. An evaluation of resources required for a compliant privacy program is underway and will include an evaluation of any required additional specialized training for users with significant privacy responsibilities.*
The CPSC has not: ✓ Performed an assessment of the knowledge, skills, and abilities of individuals with significant security and privacy responsibilities; ✓ Developed and implemented security and privacy training content; or ✓ Compiled human capital strategies to close identified gaps.	*Management concurs with this finding.* *Current practices are substantially effective. Management did not perform a formal "skills assessment" for personnel with significant security and privacy responsibilities; however, personnel with significant security or privacy roles receive appropriate training and development through formal classroom training, seminars, and mentoring.* *Documentation updates are needed to clarify interpretations.*
Management had not designed or instituted measures/metrics/exercises to assess the effectiveness of the security and privacy awareness training by the completion of the FISMA fieldwork for security/privacy training.	*Management concurs with this finding.* *Current practices are substantially effective. EXIT tracks a variety of measures associated with training effectiveness. Management measures mandatory standard and role based training completion. Blocked websites and malware are tracked and reported. Additionally management monitors the number and nature of incidents.* *Documentation updates are needed to clarify interpretations.*

Recommendations:

We recommend that management:

1. 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 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.
   - ✓ The Security Training policies and procedures should require management to provide role-based security training to users with significant security responsibilities prior to permitting these users to perform their assigned duties.
   - ✓ Management should 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. 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).

4. Include details on CPSC specific security policies and procedures in the security awareness and role-based trainings, as applicable.

5. Identify all CPSC personnel with significant privacy responsibilities and assign each of the applicable agency resources to a role (ex. SAOP, system implementer, System Owner, etc…) for training purposes.

6. Develop/purchase NIST SP 800-53, AR-5 compliant training courses for each role identified in the agency.

7. Assign personnel specialized privacy trainings commensurate with their responsibilities.

8. Establish a formal policy to require specialized privacy training for all users with significant privacy responsibilities.

9. Include details on the CPSC security policies in the privacy awareness and specialized privacy trainings, as applicable.

10. Perform a gap analysis to identify missing skills, knowledge, and abilities of individuals with significant security and privacy responsibilities.

11. Develop a remediation plan for each of the shortfalls noted in the specialized security and privacy training gap analysis.

12. Implement the remediation (training) plan for the training deficiencies identified in the specialized training gap analysis noted above.

13. Develop measures/metrics (based on the NIST SP 800-55 guidance) to assess CPSC user security and privacy awareness against and formalize those measures/metrics in CPSC policies and procedures.

14. Implement an automated solution to perform attack simulations.

15. Monitor and report the results of the new measures/metrics and the attack simulations used, to identify future training opportunities.

Identity and Access Management

The 2004 Homeland Security Presidential Directive (HSPD) 12 compels agencies to require the use of Personal Identification Verification (PIV) Cards as the common means of logical (including remote) and physical access. NIST requires agencies to establish physical and logical access policies and procedures to govern identity and access management processes. These processes include, among other requirements, the certification of user agreements, participation in various training courses, the implementation of the Principle of Least Access/Segregation of Duties, and the tracking and controlling of remote, shared, and privileged access.

Progress:
The CPSC began systematically requiring most users to utilize PIV card authentication to access agency clients in FY 2015. However, due to technical difficulties involved in the implementation, management removed the systematic controls that enforced multifactor authentication. In an effort to limit the risk associated with single factor authentication, the CPSC formally inventories, tracks, and monitors CPSC users' authentication methods. The agency is in the process of implementing a Virtual Desktop Infrastructure (VDI) and upon its full implementation (FY 2017- estimated completion) the CPSC plans to enforce PIV card access systematically. In addition, the CPSC established a formal process to authorize privileged access requests and requests to establish new-shared network accounts in FY 2015. Lastly, the CPSC is in the process of developing a new solution that will facilitate proper

segregation of duties and the principle of least access for privileged network users. The CPSC estimates by the second quarter of FY 2017, most privileged user access will be covered by this solution, and that the remaining privileged user access will be integrated into this solution within the six months following.

Issues to Be Addressed:	**Management Response:**
The agency has not implemented the Principle of Least Privilege or established proper segregation of duties for the GSS LAN. In addition, the CPSC does not define conditions for group/role membership for the GSS LAN in accordance with the CPSC Access Control Policy. For example, if a user is granted administrator access to the GSS LAN, that user can perform all security functions instead of being granted access to only those functions required by the user's job responsibilities. This results in granting users access rights that exceed their job responsibilities. Additionally, as a result of administrators being granted access on an "all or nothing" basis, they have sufficient access to access and alter the audit logs.	*Management concurs with this finding.* *Current practices are substantially effective however, because of the limited number of agency technical support staff, system privileges and duties may extend beyond optimal support boundaries.* *In FY 2016, Management implemented an access management system as the default for access to privileged system functions based on group/role membership. This solution isolates privileged access management. Access for use cases outside the default are expected to be integrated in FY 2017.*
The agency does not require separate non-privileged accounts for administrators. Instead, administrators utilize privileged accounts to perform non-privileged tasks.	*Management concurs with this finding.* *In FY 2016, Management implemented an access management system as the default for access to privileged system functions based on group/role membership. This solution isolates privileged access management. Access use cases outside the default are expected to be integrated in FY 2017.*
Management does not systematically compel all users to use a PIV card or NIST Level of Assurance 4 credential to access the network.	*Management concurs with this finding.* *Management implemented enforced PIV card authentication in 2016. PIV enforcement was temporarily suspended due to conflicts with patch management though the use of PIV or NIST Level of Assurance 4 credential remains the standard access method for system access. PIV enforcement is planned for restoration in FY 2017.*

The agency periodically reviews user account access for appropriateness, Also, it has implemented an informal process for the changing of passwords of common privileged user accounts once a user no longer requires this access, but this informal process is not consistently applied. Further, the agency policies and procedures do not require the CPSC to change passwords on shared accounts once a user with this knowledge no longer has a business need for this access. Additionally, the agency policies and procedures do not codify how quickly account passwords must be changed once a user of a common account no longer has a business need for this access. Moreover, the agency does not maintain a list of users who know the passwords to each of the common global administrator accounts.	*Management concurs with this finding.* *In FY 2016, Management implemented an access management system as the default for access to privileged system functions based on group/role membership. This solution isolates privileged access management. Access for use cases outside the default are expected to be integrated in FY 2017.*
The CPSC Access Control policy's scope does not include all agency systems. In addition, it did not adequately document the following NIST SP 800-53 requirements: ✓ How often the agency is required to review/update access control procedures. ✓ The process for revoking access in the CPSC Access Control Policy and attendant procedures is not adequately defined. Specifically, the policies/procedures do not: o document how quickly user accounts must be revoked upon notification of a change in user responsibilities; o defined the process for revoking contractor network user accounts; and o document how quickly ITDSRAM and CPSRMS user accounts must be revoked upon notification of the user's separation. ✓ Section 4.1.4 of the CPSC Access Control Policy states	*Management concurs with this finding.* *Current practices are substantially effective. The CPSC Access Control Policy covers the agency's GSS LAN—and all of the systems that are in its accreditation boundary.* *Documentation updates are needed to clarify interpretations.*

that "*The GSS LAN and all Major Applications must have defined conditions for group/role membership.*" However, the agency has not documented these conditions in a policy or procedure document for the GSS LAN. ✓ The CPSRMS access control SOP has not been updated to reflect the most recent version of NIST SP 800-53. ✓ The existing SOPs do not consistently define how the agency "*Monitors the use of information system accounts*." Specifically, the DCM access control SOP did not reference information system account monitoring and the agency has not developed an Audit and Accountability SOP for this system. ✓ The CPSC access control procedures do not adequately address the use and control of shared network and DCM accounts. Specifically, the CPSC has not established a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need for this access. In addition, the OIG noted that the Access Control policy changed on June 30, 2016 to remove the requirement for the enforcement of PIV card authentication for privileged remote access; as well as, the removal of the requirement to authorize the execution of privileged commands or access to security-relevant information via remote access.	
The CPSC does not adequately protect against and detect unauthorized remote access connections and the subversion of authorized remote access connections because the CPSC: ✓ has not developed a process to uniquely identify and authenticate endpoints prior to permitting access to the network; ✓ does not perform security scans on devices connecting remotely to the network; and	*Management concurs with this finding.* *Current practices are substantially effective. Management does have a process to authenticate endpoints prior to permitting access to the agency network. Remote access to the internal agency network is facilitated through the use of agency-controlled digital certificates that are pre-installed on all agency laptops authorized for remote access. Remote connectivity through the*

✓ does not systematically prohibit split tunneling.	*agency's virtual private network (VPN) is only approved with the detection of a valid digital certificate.*
The process to track and off-board contractors is inadequate and inconsistent. According to the Office of Resource Management (EXRM), notification to clearing officials of contractor departures in a timely manner is inconsistent. Therefore, the clearing officials cannot timely perform the tasks assigned to them (ex. revocation of the separating contractor's access). In addition, we identified 12 specific incidents where the CPSC did not immediately disable/remove information system accounts upon contractor/employee separation from the agency. In one incident, a person who had never on-boarded had an active user account. Please note the OIG identified only one instance where a non-CPSC user (this is the user who never on-boarded) had both active application user accounts and an active network account, substantially limiting the risk of this finding. Moreover, we noted one contractor who separated on 10/14/2015 that did not have his physical access to the CPSC facilities and the data center revoked.	*Management concurs with this finding.*

Recommendation:
We recommend that management: 1. Implement the Principle of Least Privilege and establish proper segregation of duties for the GSS LAN by: ✓ Defining and documenting the functions/duties, which have a significant impact on agency operations, and creating roles that systematically separate the users' ability to perform these functions. ✓ Revoking access to all users who have access to the functions beyond their mission need. ✓ Reviewing the logs of all admin/super user accounts and restricting this access if the levels of privilege are not specifically

necessary to perform the user's required job functions.

- ✓ Documenting the new 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.).

2. Implement a solution, which allows the agency to report on/restrict 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. Periodic audits should be performed to ensure access remains appropriate.

3. Limit administrators' access to update audit logs and implement a solution to monitor changes to the audit logs and notify the CSIRT team in the event of an audit log modification.

4. Identify and formally authorize all known Segregation of Duties and least access issues. Actively implement a solution to monitor tasks performed by resources with approved conflicting duties.

5. Create separate non-administrative user accounts for administrators, and require administrators to use these accounts when performing tasks that do not require administrative privileges.

6. Grant administrators local administrative accounts to each privileged service individually, instead of using the global system administrator accounts. Administrators should check-in/check-out the privileged services only when this access is required and this access should be logged and monitored.

7. Systematically compel PIV card authentication for all users accessing CPSC systems.

8. Implement a formal process:

- ✓ To identify, limit and control the use of shared user accounts.
- ✓ To maintain a comprehensive inventory of users who know the passwords to shared accounts.
- ✓ To require the CPSC to change the credentials on all shared user accounts whenever a user with knowledge of these credentials separates from the CPSC or changes job functions and no longer requires access to the account.
- ✓ To eliminate the use of global administrator accounts and provision uniquely identifiable user accounts to perform limited administrative tasks based on documented business needs.
- ✓ To require periodic password changes on all common accounts.

9. Develop logical access control policies and procedures for all agency systems. This may be achieved by establishing an entity-wide logical access policy for agency systems and procedure documents that establish rules for the individual systems, where applicable.

10. Provide training to individual system owners, where necessary, on how to establish, implement, and maintain logical access policies and procedures for systems that do not currently have policies and procedures.

11. Update the CPSC Access Control Policy and attendant procedures to include:
    - ✓ A process that adequately defines revoking user access. Specifically, the agency should document:
        - How quickly user accounts must be revoked upon notification of a change in user responsibilities;
        - The process for revoking contractor network user accounts;
        - How quickly ITDSRAM and CPSRMS user accounts must be revoked upon notification of the user's separation;
    - ✓ Defined conditions for group/role membership within the GSS LAN;
    - ✓ The CPSRMS access control SOP should be based on NIST SP 800-53 Rev 4 rather than NIST SP 800-53, Rev. 3;
    - ✓ The DCM access control SOP should reference information system account monitoring and the CPSC should develop an Audit and Accountability SOP for DCM;
    - ✓ A process that adequately addresses the use and control of shared network and DCM accounts. Specifically, the CPSC should establish a process for reissuing shared account credentials when individuals separate from the agency or when they no longer have a business need for this access;
    - ✓ A requirement for the enforcement of PIV card authentication for remote access;
    - ✓ A requirement for the restriction of the execution of privileged commands and access to security-relevant information via remote access;
    - ✓ References to individual system access control SOPs and the shared and privileged account request authorization SOPs.

12. Implement a network access control solution to authenticate devices prior to allowing access to the network.

13. Systematically restrict split tunneling.

14. Perform security scans on devices connecting to the CPSC network prior to allowing access to the network.

15. Revoke separated users' access to CPSC facilities and all relevant information systems.

16. Implement a centralized contractor database with automated workflow to track the on and off boarding of contractors.

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

18. Configure CPSRMS to revoke accounts after 30 days of inactivity or revoke CPSRMS users upon the disabling (not just deleting) of users' network accounts.

19. Train the Contracting Officer Representatives (CORs), EXRM, and EXIT resources responsible for processing contractor separations on their respective contractor separation responsibilities.

20. Require a periodic review of contractor status by the CORs and coordinated by EXRM or Procurement; and

21. Provide the EXIT representatives and the relevant program officials with a weekly report of contractor separations. The agency 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 2016. The requirements of the review included:

- Evaluating and testing the internal controls defined in the 2016 FISMA metrics (provided by DHS);
- Assessing whether the CPSC's information security policies, procedures, and practices comply with the Federal laws, regulations, and policies outlined in the 2016 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 2016 FISMA reporting metrics developed by DHS dated September 26, 2016 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 2016 to October 2016 at the CPSC's headquarters, located in Bethesda, Maryland. The OIG focused this evaluation within the boundaries of the GSS LAN, CPSRMS, DCM, 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 Risk Management and POAM processes to ensure that all security weaknesses are identified, tracked, and addressed;
(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 and privacy training, contractor systems, and contingency planning.
(4) The statuses of each of these topics were reviewed and discussed with the CPSC's CIO, Director of Technical Services (ITTS), Chief Information Security Officer (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
- ✓ backup reports
- ✓ employee and contractor rosters
- ✓ MOUs & ISAs
- ✓ planning documentation
- ✓ vulnerability reports and system scanning results
- ✓ change control forms
- ✓ risk documentation
- ✓ security/privacy training content/reports
- ✓ system configurations
- ✓ contingency plans
- ✓ system inventories
- ✓ agency templates
- ✓ contracts and Statement Of Works
- ✓ meeting minutes

This evaluation constitutes both a follow-up of the findings and recommendations resulting from earlier reviews and a review of the CPSC's implementation of the IT security criteria, as currently defined by FISMA.

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

APPENDIX C: CRITERIA

Center for Internet Security (CIS)
The CIS Critical Security Controls for Effective Cyber Defense (v6.0)

Chief Acquisition Officers (CAO)/CIO Council
Best Practices for Acquiring IT as a Service

Department Of Homeland Security (DHS):
2016 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*
OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*
OMB M-16-04, *Cybersecurity Strategy and Implementation Plan*

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

National Archives and Records Administration (NARA)
General Schedule

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

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

General Services Administration (GSA)
Federal Acquisition Regulation

APPENDIX D: ACRONYMNS & ABBREVIATIONS

Acronym/Abbreviation	Description
ATO	Authorization to Operate
BIA	Business Impact Analysis
BCP	Business Continuity Plan
CAO	Chief Acquisition Officers
CFR	Code of Federal Regulations
CIGIE	Council of Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
COOP	Continuity Of Operation Plan
COR	Contracting Officers Representative
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
DHS	Department of Homeland Security
DOI	Department of the Interior
DR Plan	Disaster Recovery Plan
EXIT	Office Of Information Technology
EXRM	Office of Resource Management
FAR	Federal Acquisition Regulation
FCD1	Federal Continuity Directive 1
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FMPS	Office of Procurement Services
FY	Fiscal Year
GISRA	Government Information Security Reform Act
GSS LAN	General Support System Local Area Network
HSPD 12	Homeland Security Presidential Directive 12
IR	Incident Response
ISA	Interconnect Security Agreement
ISCM	Information System Continuous Monitoring
ISCP	Information System Contingency Plan
ITTS	Information Technology and Technical Services
ITDSRAM	International Trade Data System/Risk Automation Methodology System
MOU	Memo Of Understanding
NARA	National Archive and Records Administration
NIST	National Institute of Standards and Technology

NVD	National Vulnerability Database
OGC	Office of the General Counsel
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
SaaS	Software-as-a-Service
SAR	Security Assessment Report
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOD	Segregation of Duties
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TIC	Trusted Internet Connection
TT&E	Training, Testing and Exercises
UII/UPI	Unique Investment Identifiers/Unique Project Identifiers
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VDI	Virtual Desktop Infrastructure

APPENDIX E: MANAGEMENT RESPONSE

Page was intentionally left blank

UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
4330 EAST WEST HIGHWAY
BETHESDA, MD 20814

Memorandum

Date: December 9, 2016

TO : Christopher Dentel
Inspector General
Office of the Inspector General

THROUGH: Patrick Manley
Chief Information Security Officer
Office of Information and Technology Services (EXIT)

FROM : James Rolfes
Assistant Executive Director/ Chief Information Officer
Office of Information and Technology Services (EXIT)

SUBJECT : Management Response to FY 2016 Evaluation of the CPSC's Federal Information Security Act (FISMA) Implementation

Thank you for the opportunity to review and provide a management response for your FY 2016 FISMA evaluation. The Office of Information and Technology Services has continued to improve the IT security program over the course of the past year. Some of the accomplishments included:

- Performed substantial work in support of agency IT Security and Information Assurance
  - Blocked approximately
    - 1,200 instances of malware
    - 1.2 million spam messages
    - Addressed 15,377 vulnerabilities across all systems
  - Developed or updated 20 different IT security policy documents
  - Developed SOPs for organization Risk Acceptance, Risk Assessment processes, and security impact assessment
  - Completed assessments for over 70 agency minor applications
  - Implemented monthly database, VMware, and network printer scanning
  - Implemented website vulnerability scanning
  - Completed agency's Cloud –based FedRAMP ATO for the Drupal System
  - Migrated agency security management activities to the DOJ CSAM system—allowing improved tracking and visibility of agency POAMs, security plans, and assessments

    - Improved configuration management practices by implementing continuous database scanning and reporting
- Completed 100 percent of required Security Impact Assessments (SIA) and Privacy Impact Assessments (PIA) on time
- Completed 100 percent of agency reauthorization Authority to Operate (ATO) documents the GSS LAN and each Major Application on time
- Oversaw improvements in monthly security reporting, POAM reviews, monthly vulnerability scanning. Reduced agency POAM backlog by 47%
- Oversaw completion of three different security audits: PII, FISMA, independent. Provided substantial support for agency financial audit
- Completed formal interagency security agreements for the Hotline Support and PRISM support contracts

EXIT has carefully reviewed the evaluation and generally concurs with the findings with the exception of the finding indicating that CPSC's inventory of major applications is incomplete. We reviewed the sources referenced by the OIG including the requirements in OMB Circular A-130 and M -10-15 *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* and believe that our major application inventory is consistent with that guidance. Additionally, EXIT reviewed the guidance provided in NIST 800-18 rev 1 *Guide for Developing Security Plans for Federal Information Systems* which includes guidance on system security planning roles and system boundary analysis. EXIT believes its current major application inventory and general support systems designations are consistent with this guidance.

EXIT believes that including important context regarding the OIG's findings provides additional information about CPSC's security posture. Therefore, in this Management Response, EXIT added context to help characterize the risk impacts for each finding.