Office of Inspector General

U.S. Consumer Product Safety Commission

Evaluation of CPSC's FISMA Implementation for FY 2018

October 31, 2018

Vision Statement

We are agents of positive change striving for continuous improvements in our agency's management and program operations as well as within the OIG.

Statement of Principles

We will:

Work with the Commission and the Congress to improve program management;

Maximize the positive impact and ensure the independence and objectivity of our audits, investigations, and other reviews;

Use our investigations and other reviews to increase Government integrity and recommend improved systems to prevent fraud, waste, and abuse;

Be innovative, question existing procedures, and suggest improvements;

Build relationships with program managers based on a shared commitment to improving program operations and effectiveness;

Strive to continually improve the quality and usefulness of our products; and

Work together to address Government-wide issues.

Office of Inspector General
U. S. CONSUMER PRODUCT SAFETY COMMISSION

October 31, 2018

TO: Ann Marie Buerkle, Acting Chairman
Robert S. Adler, Commissioner
Elliot F. Kaye, Commissioner
Dana Baiocco, Commissioner
Peter A. Feldman, Commissioner

FROM: Christopher W. Dentel, Inspector General Christopher W. Dentel

SUBJECT: Evaluation of CPSC's FISMA Implementation for FY 2018

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.

To assess agency compliance with FISMA for FY 2018, we retained the services of Richard S. Carson & Associates, Inc. (Carson), a security and management consulting firm. Under a contract monitored by the OIG, Carson issued an evaluation report regarding the CPSC's compliance with FISMA. The contract required that the evaluation be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation.

In evaluating the CPSC's progress in implementing its agency-wide information security program, Carson specifically assessed the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security and the Office of Management and Budget.

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 17 findings and 52 recommendations 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.

Table of Contents

Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency as a whole.

FISMA requires the annual evaluation to be performed by the agency's Office of Inspector General (OIG) or by an independent external qualified contractor under OIG monitoring. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated data collection tool, CyberScope.

The U.S. Consumer Product Safety Commission (CPSC) OIG retained Richard S. Carson & Associates, Inc. (Carson) to perform an independent evaluation of the CPSC's implementation of FISMA for Fiscal Year (FY) 2018. This report serves to document the CPSC's compliance with the requirements of FISMA. In evaluating the CPSC's progress in implementing its agency-wide information security program, we specifically assessed the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security (DHS) and OMB.

What We Found

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements. The CPSC has continued to focus its efforts on the implementation of the following processes/systems:

- [redacted]
- Development of a formal Enterprise Architecture (EA). The agency's focus is currently on bootstrap data management and requirements as outlined via the Federal Enterprise Architecture (FEA).
- Engagement with stakeholders in support of the establishment of an Executive Risk function, led by the CPSC Chief Financial Officer (CFO) and including the Chief Information Officer (CIO), the Chief Information Security Officer, and various mission executives for adoption of information security related processes.
- The security and awareness training and role-based training program.
- The Information Security Continuous Monitoring (ISCM) program.

We noted seventeen (17) 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.

What We Recommend

To improve the CPSC's implementation of FISMA, we make 52 recommendations.

1. OBJECTIVE

The objective was to perform an independent evaluation of the CPSC's implementation of FISMA for FY 2018.

2. BACKGROUND

On December 18, 2014, the President signed FISMA, which reformed the Federal Information Security Management Act of 2002. FISMA outlines the information security management requirements for agencies, which includes an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency as a whole. FISMA requires the annual evaluation to be performed by the agency's OIG or by an independent external qualified contractor. OMB Memorandum 18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 16, 2017, requires the OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via CyberScope.

The CPSC OIG retained Carson to perform an independent evaluation of the CPSC's implementation of FISMA for FY 2018. This report presents the results of that independent evaluation. Carson will also prepare responses to OMB's annual FISMA reporting questions for OIGs, and the CPSC OIG will submit this information via OMB's automated collection tool in accordance with OMB guidance.

3. CRITERIA

Carson utilized the criteria established by the federal government to evaluate the CPSC's FY 2018 IT security program in accordance with FISMA. For a complete listing of criteria, refer to Appendix A.3.

4. EVALUATION RESULTS

Based on the government-wide OIG metric requirements, we concluded that the CPSC has continued to make improvements in its IT security program and progress in implementing the recommendations resulting from previous FISMA evaluations.

We attributed many of the issues that we identified to the CPSC's decision to not dedicate the resources necessary to support the implementation of planned activities.

5. FINDINGS

5.1 FINDING 1: LACK OF COMPLETED ASSESSMENT AND AUTHORIZATION (A&A) PACKAGES FOR MAJOR SYSTEMS WITH SIGNED AUTHORITY TO OPERATE (ATO)

Condition

The CPSC has not completed a comprehensive assessment of all of its major systems and attested to the systems' security controls meeting the established security requirements. The organization has not followed its internal processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for all of its major systems. Based on the lack of completed A&A packages and signed ATOs, it could not be determined if management effectively performed appropriate system-level risk assessments, security control selections, or if management applied an acceptable risk assessment methodology to tailor the set of selected controls.

Criteria

FISMA requires an assessment of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.

The National Institute of Standards and Technology (NIST) develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.

NIST Special Publication (SP) 800-37 Revision (Rev) 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, provides guidance to federal agencies for authorizing information systems and maintaining a current and valid security accreditation.

NIST Supplemental Guidance on Ongoing Authorization, provides additional guidance which amplifies the current NIST guidance on security authorization and ongoing authorization contained in SPs 800-37, Rev 1; 800-39; 800-53, Rev 4; 800-53A; and 800-137.

Cause

Annual security assessments of major systems were not timely completed by the assessor contracted to perform the CPSC's annual independent security assessment, Department of the Interior.

Effect

Failure to independently assess all major systems' security controls may lead to management not fully understanding the risks posed by operating these systems.

Recommendation

We recommend management:

1. Obtain completed annual A&A packages with valid ATO for all of the CPSC's major systems.

5.2 FINDING 2: LACK OF ENFORCEMENT OF PERSONAL IDENTITY VERIFICATION (PIV) ACROSS THE ORGANIZATION

Condition

The CPSC has made progress in implementing Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, and now enforces PIV card authentication systematically for the vast majority of its users. [redacted]

[redacted]

[redacted]

Criteria

OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

The Cybersecurity Strategy and Implementation Plan, published by the OMB on October 30, 2015, requires that federal agencies use PIV credentials for authenticating privileged users.

Federal Information Processing Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, defines the technical requirements for a common identity.

NIST SP 800-63, Rev 3, *Digital Identity Guidelines*, provides guidance around the utilization of strong authentication mechanisms.

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

- [redacted]

5.3 FINDING 3: INADEQUATE IMPLEMENTATION OF AN INFORMATION SYSTEM INVENTORY AND AN INFORMATION SYSTEM COMPONENT (ASSET) INVENTORY

Condition

The CPSC has developed an information system inventory that includes information systems designated as “major” and “minor.” However, the CPSC has not documented the process for defining a major information system based on criteria outlined in OMB Circular A-130 (e.g., mission, costs, or significant role). For example, OMB Circular A-130 defines a major information system as one that requires special management attention because it has a significant role in the administration of an agency’s programs, finances, or property.

However, the CPSC has not designated their property management systems as major information systems.

The CPSC has implemented various tools to develop a comprehensive information system component inventory including a property management system for tracking physical assets; a network asset management solution that scans the CPSC network for hardware and software assets; and a vulnerability scanner which also scans the network for connected devices. However, the following areas have not been addressed by the CPSC:

- Management of software license inventory is currently manual, informal, and performed on an ad hoc basis.

- [redacted]
- Standard data elements (taxonomy) have not been defined and documented to support the existing asset inventory in accordance with FEA Framework.
- [redacted]

Criteria

FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under control of the agency. The inventory must be updated at least annually and used to support information resource management.

OMB Circular A-130 defines a “major information system” as a system that is part of an investment that requires special management attention as defined in OMB guidance, a “major automated information system” as defined in 10 United States Code § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11, Capital Programming Guide.

NIST SP 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to develop and maintain an inventory of its information systems, as well as inventory of all components within the authorization boundary of each information system.

Additionally, NIST SP 800-53, Rev 4 requires the following:

- Continuous monitoring program to facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.
- Inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary, and is at a level of granularity deemed necessary for tracking and reporting.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, further outlines requirements for the security-related information pertaining to a system component inventory.

Cause

The CPSC has taken steps to improve its information system inventory as well as its hardware and software asset management processes. However, it has not dedicated the resources necessary to formalize and implement policies and procedures that are sufficient to adequately govern its hardware and software asset inventory.

Effect

The CPSC not having accurate and up-to-date hardware, software, and system inventories indicates that the CPSC does not have a clear understanding of their system environment, or the risk associated with that environment. [redacted]

Recommendation

We recommend management:

3. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance.
4. Develop, document, and implement a process to classify agency systems as “major” or “minor” in accordance with OMB Circular A-130.
5. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications.
6. [redacted]
7. Define and document the taxonomy of CPSC’s systems to be classified as one of the following types: IT system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC’s operational mission, facility, or social media) in accordance with FEA.
8. [redacted]

5.4 FINDING 4: LACK OF ENFORCEMENT AROUND THE PRINCIPLE OF LEAST PRIVILEGE AND/OR SEPARATION OF DUTIES FOR PRIVILEGED ACCOUNTS

Condition

The CPSC does not apply account management controls to support the Principle of Least Privilege and management of temporary and emergency accounts. In 2016, the CPSC initiated the implementation of an automated privileged access management solution to address known issues around compliance with the Access Control Policy. The CPSC continues with its efforts to fully implement this solution. However, the CPSC has not adequately defined all of its identity and access policies and procedures or implemented the following:

- Proper segregation of duties and the implementation of the Principle of Least Access.

[redacted]

[redacted]

- Automatic revocation of temporary and emergency accounts after a specified period of time.
- A process to ensure privileged account credentials are managed in accordance with NIST SP 800-53, Rev 4, Identification and Authentication-5 (IA-5).

Criteria

NIST SP 800-53, Rev 4 requires the organization to develop, document, and distribute access control policy and procedures which define the processes in place for the following:

- [redacted]
- [redacted]
- The application of Segregation of Duties and the Principle of Least Access.
- Removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed.

Cause

[redacted]

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

9. [redacted]
10. [redacted]

11. Define and implement identification and authentication policies and procedures.
12. Automatically revoke temporary and emergency access after a specified period of time.

5.5 FINDING 5: LACK OF DEFINED STRATEGY AND MILESTONES TO ALIGN WITH FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) AND IMPLEMENTATION OF DHS'S CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) PROGRAM

Condition

The CPSC Access Management Plan provided adequately supports the requirement for CPSC users to utilize PIV cards to access agency resources. [redacted] However, the CPSC was unable to provide a strategy with milestones for the implementation of FICAM segment architecture and phase 2 of DHS's CDM program.

Criteria

FICAM provides a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government.

Cause

Management has not dedicated the appropriate resources to develop a proper strategy for implementing FICAM's segment architecture. Additionally, direction from DHS is required to support a robust CDM implementation.

Effect

A lack of defined milestones for the development of the FICAM segment architecture and CDM implementation may lead agency systems to be compromised.

Recommendation

We recommend management:

13. Define and document a strategy (which include specific milestones) to implement FICAM.
14. Integrate ICAM strategy and activities into the enterprise architecture and ISCM.

5.6 FINDING 6: ROLE-BASED TRAINING REQUIREMENTS AROUND SECURITY AND PRIVACY ARE NOT ADEQUATELY DEFINED ACROSS THE ORGANIZATION

Condition

The CPSC’s Awareness and Training Policy outlines requirements for EXIT IT staff, and this policy has been implemented fully. The CPSC’s electronic training solution maintains training records for all CPSC personnel. However, the policy does not require non-IT staff to complete role-based training, and role-based training is not provided to these individuals. Based on requirements outlined in Code of Federal Regulations (CFR) 5 CFR 930.301, role-based training must be provided to all personnel that affect security, which includes members of the Risk Executive Function and all other applicable roles described in the CFR, in addition to all other applicable roles at the CPSC outlined in this CFR.

The agency-specific policies, procedures, and responsibilities were not defined within the security awareness or role-based trainings provided by management. Additionally, the CPSC could not demonstrate that it has performed an adequate assessment of the knowledge, skills, and abilities of its workforce with significant security responsibilities. Therefore, the content of security awareness and specialized training has not been tailored adequately to reflect the CPSC’s organization, requirements, types of systems, culture, mission, and risk environment.

Criteria

NIST SP 800-53, Rev 4 requires the development and documentation of security awareness and training policy and supporting procedures. This guidance also requires the dissemination of this policy and procedures to stakeholders, and that the policy and procedures should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

As codified in 5 CFR 930.301, all roles that affect security must be provided role-based security training. These roles include: executives, program and functional managers, Chief Information Officers, IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers), IT function management, and operations personnel.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization’s IT security program.

Cause

Management has not documented and implemented a training program that requires all individuals with significant security responsibilities be provided role-based training in accordance with the CFR.

Effect

Management has not adequately identified the personnel required to complete specialized or role-based training, increasing the risk of improper actions and/or decision making. Additionally, inadequate training increases the risk of the improper implementation of agency-defined policies and procedures.

Recommendation

We recommend management:

15. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security and privacy (e.g., Executive Risk Council) are required to participate in role-based and/or specialized training.
16. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities.
17. Develop/tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals.

5.7 FINDING 7: LACK OF DEFINED AND COMMUNICATED SECURITY CONTROL IMPLEMENTATION AND ISCM ACTIVITIES

Condition

The CPSC has defined processes for performing assessments, authorizations, and monitoring for ISCM. The CPSC ISCM Plan defines the assessment frequency, ranging from 1 to 5 years, for each security control, as well as the monitoring frequency (e.g., monthly, quarterly, semi-annually, annually) for security controls that require continuous monitoring. The CPSC ISCM Plan also includes a schedule for performing annual assessments through FY2020. However, the CPSC has not documented the establishment or assessed the implementation of all relevant security controls associated with all agency-defined major systems. For example, the CPSC has not conducted a security assessment of the privacy controls specified in NIST SP 800-53, Rev 4, Appendix J. In addition, the CPSC ISCM Plan does not specify the assessment frequency, monitoring frequency, or annual testing schedule for the program management family (PM) of security controls and for the privacy controls.

The CPSC utilizes the CPSC General Support System Local Area Network (GSS LAN) System Security Plan (SSP) as its organization-wide information security program plan. The CPSC GSS LAN SSP includes references to the Program Management controls required by NIST SP 800-53, Rev 4; however, they are not adequately documented. The implementation statements included in the SSP were not all properly parameterized or sufficient to facilitate an assessment of the effectiveness of these controls.

In addition, the security controls descriptions in the CPSC GSS LAN SSP do not include any indication of which controls are common controls, and for those controls that are common controls (e.g., the PM controls), who is responsible for their implementation.

Criteria

FISMA requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security Program Management family of controls are described in NIST SP 800-53, Rev 4, Appendix G. These controls should be implemented at the organizational level (i.e., common controls).

NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, also requires the development, documentation, and dissemination of policies and procedures across the organization. Additionally, procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls are required.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, states that common security controls should be documented once, and that the individual responsible for implementing the common control should be listed in the security plan. Descriptions of security controls in a security plan should include 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been considered and applied; and 4) indicate if the security control is a common control and who is responsible for its implementation.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, provides guidelines for applying the Risk Management Framework to federal information systems, which includes conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring (e.g., ISCM).

Cause

Management has not allocated the resources necessary to define a comprehensive ISCM Plan or to perform assessments of all required security controls.

Effect

This limits management awareness of the information security risk associated with agency information and information systems.

Recommendation

We recommend management:

18. Perform a gap analysis to identify all NIST SP 800-53, Rev 4 security controls that were not documented and assessed.
19. Document the implementation of all relevant security controls identified in the gap analysis.
20. Assess the implementation of all relevant security controls that were identified in the gap analysis.
21. Update the implementation statements for the program management family of controls in the GSS LAN SSP to facilitate an assessment of the effectiveness of those controls.
22. Update the GSS LAN SSP to clearly indicate which controls are common controls, and who is responsible for their implementation.
23. Update the CPSC ISCM Plan to specify the assessment frequency, monitoring frequency, and annual assessment testing schedule for the program management family of security controls, and the privacy controls.

5.8 FINDING 8: NO EXISTING ENTERPRISE ARCHITECTURE DOCUMENTED FOR MANAGING RISK

Condition

Although the CPSC has documented a Risk Management Framework, the CPSC has not defined an EA and integrated the EA into the agency's risk management strategy; therefore risk is not managed from an organizational level.

Criteria

In response to FISMA requirements, NIST developed and published SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, to provide guidance for an integrated, organization-wide program for managing information security risk.

NIST SP 800-53, Rev 4 requires federal organizations to:

- Develop an information security architecture.
- Review and update the information security architecture in accordance with the enterprise architecture.
- Ensure planned information security architecture changes are appropriately aligned with security plans, Concept of Operations (better known as CONOPS), and organizational procurements/acquisitions.
- Manage the information system using the system development life cycle (SDLC) employing security considerations.
- Define and document information security roles and responsibilities throughout the SDLC.
- Identify personnel with designated security roles and responsibilities.
- Integrate the organizational information security risk management process into SDLC activities.
- Apply security engineering principles in the specification, design, development, implementation, and modification of information systems.

FEA provides the federal government with a common approach for the strategic integration of business and technology management. Implementation of the FEA requires a description of current structures and behaviors within an organization to support planning and decision making to better align with established goals and strategic direction.

Cause

Management has taken an alternative approach for implementing an EA by focusing on data gathering, which has delayed the implementation of NIST controls and the Federal Enterprise Architecture Framework.

Effect

The lack of a defined current and target state EA may foster inconsistent management of risk across the organization, ultimately impacting the CPSC's mission success.

Recommendation

We recommend management:

24. Develop an EA to be integrated into the risk management process.

5.9 FINDING 9: INSUFFICIENT DOCUMENTATION AROUND CONFIGURATION MANAGEMENT

Condition

The CPSC relies on the GSS LAN Configuration Management policy and has documented a configuration management procedure. However, management has not fully implemented the Configuration Management (CM) policies and procedures. Also, no organizational-specific CM plan has been established and implemented to support the policy. As such, the CPSC has not documented a process for identifying configuration items throughout the system development life cycle and managing the integration of the configuration items.

The CPSC has not adequately developed, documented, and disseminated policies and procedures that describe the processes used by management to develop common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has not established a deviation process.

[redacted]

The CPSC has not defined and documented all the Trusted Internet Connections (TIC) critical capabilities that it manages internally.

Criteria

FISMA requires an assessment of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.

NIST SP 800-53, Rev 4 requires the organization to develop, document, and disseminate configuration management policy and procedures; current baseline configurations; and configuration change controls for organizational information systems. Additionally, NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, provides guidance focusing on the implementation of the information system security aspects of CM.

In response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, the Cybersecurity Framework (CSF) was established in part to foster risk and cybersecurity management communications. The Cybersecurity Framework is mapped to NIST 800-53, Rev 4 and the SANS Top 20 set of controls.

Center for Internet Security Control 3.7, has been mapped as a measure to establish, implement, and actively manage the security configuration of IT assets using configuration management and change control process in an effort to prevent attackers from exploiting vulnerable services and settings.

Cause

Management has not dedicated the resources required to adequately develop, document, and implement adequate CM processes.

Effect

Without a developed, documented, and communicated set of CM procedures, the CPSC risks not maintaining the integrity and availability of assets supporting the mission of the organization.

Recommendation

We recommend management:

25. Develop and enforce a CM plan that includes all requisite information.
26. Develop and implement a set of CM procedures in accordance with the inherited CM Policy which includes appropriate measures for all hardware, software, and supporting infrastructure (e.g., equipment, networks, and operating systems).
27. [redacted]
28. Further define the resource designations for a Change Control Board.
29. Identify and document the characteristics of items that are to be placed under CM control.
30. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of changes.
31. [redacted]
32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service.

5.10 FINDING 10: LACK OF FORMALLY DOCUMENTED CONTINGENCY PLANS

Condition

The CPSC was unable to provide a formally documented set of Contingency Plans that included an organization-wide Continuity of Operations Plan (COOP) and

Business Impact Assessment (BIA), Disaster Recovery Plan, Business Continuity Plans (BCPs), and Information System Contingency Plans (ISCPs). Based on this lack of documentation, it was determined that the CPSC has not documented or assessed the contingency steps required to recover agency systems and processes to support the CPSC mission in the event of a disruption. Therefore, the effectiveness of the following could not be supported:

- Maintenance and integration with other continuity areas to include organization and business process continuity, disaster recovery planning, and incident management.
- Integration of contingency planning with the Enterprise Risk Management (ERM) program.
- Specialized training activities for designated appropriate teams responsible for implementing the contingency plan strategies.
- Testing and exercises as integrated with Incident Response Plan (COOP/BCPs).

Also, the CPSC has completed BIAs for existing major systems. However, as noted above, an organizational BIA has not been completed and/or distributed.

Additionally, supporting standard operating procedures for the major systems have not been developed and distributed.

Criteria

NIST SP 800-53, Rev 4 requires the organization to develop, maintain, and integrate the plan with other continuity plans.

Additionally, NIST SP 800-34, Rev 1, *Contingency Planning Guide for Federal Information Systems*, provides guidance to assist organizations with evaluating information systems and operations to determine contingency planning requirements and priorities. Functions organize basic cybersecurity activities at their highest level. These functions are: Identify, Protect, Detect, Respond, and Recover.

NIST CSF, *Framework for Improving Critical Infrastructure Cybersecurity*, provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. CSF provides a set of activities to achieve specific cybersecurity outcomes which organize basic cybersecurity activities at their highest level into the same five functions listed earlier: Identify, Protect, Detect, Respond, and Recover.

Federal Continuity Directive 1 (FCD1), *Federal Executive Branch National Continuity Program and Requirements*, provides implementation requirements to establish a continuity program and planning for executive departments and agencies. The required elements include the delineation of essential functions; succession to office and delegations of authority; safekeeping of and access to essential records; continuity locations; continuity communications; human resources planning; devolution of essential functions; reconstitution; and program validation through testing, training, and exercises.

National Archives and Records Administration (NARA), General Records Schedules, Section 3.2, Information Systems Security Records, provides federal agencies with the required schedules for the protection of security related information and data.

Cause

Management has not dedicated the resources required to adequately develop and document an effective process to recover agency systems and processes to support the CPSC mission in the event of a disruption.

Effect

Without a developed, documented, and communicated set of contingency plans and processes, the CPSC risks not being able to recover agency systems and processes to support the CPSC mission in the event of a disruption.

Recommendation

We recommend management:

33. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (e.g., NIST SP 800-34/53, FCD1, NIST CSF, and NARA guidance).
34. Develop, document, and distribute all required Contingency Planning documents (e.g., organization-wide COOP and BIA, Disaster Recovery Plan, BCPs, and ISCPs) in accordance with appropriate federal and best practice guidance.
35. Test the set of documented contingency plans.
36. Integrate documented contingency plans with the other relevant agency planning areas.

5.11 FINDING 11: MEDIA SANITIZATION DISPOSAL PROCEDURES

Condition

The CPSC has established procedures to sanitize information system media prior to disposal, release out of organizational control, or release for reuse. The CPSC utilizes a disk wipe utility to sanitize disk drives, as well as shredders and locked containers to protect data. However, the procedures are not documented around how media should be sanitized prior to disposal.

Additionally, [redacted]

Criteria

NIST SP 800-53, Rev 4 requires the organization to develop, document, and disseminate procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

37. Develop, document, and distribute all required procedures for the destruction or reuse of media containing PII or other sensitive agency data (e.g., proprietary information).

[redacted]

5.12 FINDING 12: CONTRACT LANGUAGE DOES NOT ADEQUATELY IDENTIFY REQUIREMENTS TO MITIGATE RISKS

Condition

The CPSC has developed a standard operating procedure that outlines the requirement for agency Contracting Officer Representatives and EXIT to coordinate with the Division of Procurement Services (FMPS) to ensure the appropriate Federal Acquisition Regulations (FAR) clauses are included in agency contracts for all “incoming requisition procurement packages.” But, the CPSC has not documented, in a policy or procedures, an approach to ensure that existing contracts and other agreements for third party systems and services include all appropriate IT security clauses. In addition, management has not defined or implemented an approach to ensure that all NIST SP 800-53, Rev 4, Security Assessment-4 (SA-4) or cloud computing requirements are included in agency contracts. Moreover, the CPSC has not defined its processes to ensure that security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.

The CPSC has not updated existing IT contracts and/or agreements to include the requirements outlined in the CIO/Chief Acquisition Officer's Council's Cloud Computing Contract Best Practices or the following FAR clauses, and NIST requirements:

- FAR 39.105, Privacy
- FAR 39.101, Policy
- FAR 52.224-1, Privacy Act Notification clause
- FAR 52.224-2, Privacy Act clause;
- FAR 52.239-1, Privacy or Security Safeguards
- NIST SP 800-53, Rev 4, SA-4 requirements

Criteria

NIST SP 800-53, Rev 4 requires the inclusion of acceptance criteria for information systems, information system components, and information system services. These requirements must be defined in the same manner as criteria for any other organizational acquisition or procurement and must include references to the FAR.

Cause

EXIT and FMPS have not effectively collaborated to ensure the inclusion of required FAR clauses and NIST requirements into new contracts and to update existing contract clauses as conditions change.

Effect

Missing security and privacy clauses from obligating documents introduces and increases the risk of security weaknesses to the CPSC arising from the service provider not being contractually required to meet security and privacy requirements.

Recommendation

We recommend management:

40. Establish and implement policies and procedures to require coordination between EXIT and FMPS to facilitate identification and incorporation of the appropriate contract clauses within all contracts.

5.13 FINDING 13: RISK FROM AN ORGANIZATIONAL LEVEL IS NOT ADEQUATELY MANAGED

Condition

Management has acquired resources to support the development of an organizational risk management plan. However, the CPSC has not formally documented a strategy for defining and applying risk tolerance at the organizational level. Therefore, the risk profile that drives the determination of the types of risk that management is willing to assume, at an organizational level, has not been adequately defined.

The following activities also cannot be deemed as effectively implemented:

- Capturing and sharing of the lessons learned on the effectiveness of risk management processes and activities required to update and improve the program.
- Collection of qualitative and quantitative performance measures on the effectiveness of the risk management strategy.
- Scenario analysis and modeling of potential responses.

Additionally, the CPSC has not developed an ERM program (as outlined by the CFO Council's *ERM Playbook*) or prioritized missions/business functions at the organizational level.

Criteria

NIST SP 800-53, Rev 4 requires the organization to implement the following criteria:

- Define critical infrastructures and resources.
- Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations.
- Implement a risk management strategy consistently across the organization.
- Review and update the risk management strategy on a periodic basis to address organizational changes.

NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, provides guidance around managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. This publication adheres to requirements of OMB Circular A-130, *Appendix III, Security of Federal Automated Information Resources*.

The CFO Council ERM Playbook provides high-level key concepts for consideration when establishing a comprehensive and effective ERM program and aligns with guidelines presented via OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

Cause

The CPSC has not prioritized the completion of organization-level risk assessments to date.

Effect

Without a strategy in place to rank and quantify agency risks against mission and strategic objectives, the CPSC cannot efficiently and effectively direct resources to the agency's most critical challenges.

Recommendation

We recommend management:

41. Develop and implement an ERM program based on NIST guidance and guidance from the ERM Playbook (A-123, Section II requirement). This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC.
42. Identify, document, and implement a strategy to determine the organizational risk tolerance and adequately document the approach in the risk management strategy, policies, and procedures.
43. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.

5.14 FINDING 14: PLAN OF ACTIONS AND MILESTONES (POA&MS) ARE NOT ADEQUATELY DOCUMENTED AND IMPLEMENTED

Condition

The CPSC has not established and implemented policies and procedures that require agency personnel to capture all of the OMB required information in the CPSC POA&Ms. For example, based on the April 2018 POA&Ms, 178 of 211 (84%) weaknesses are missing estimated funding resources. In addition, the CPSC does not include key milestones with completion dates for each weakness and does not track changes to milestones. For example, of the 211 weaknesses on the April 2018 POA&Ms, 82 are delayed more than 2 years; however, there is no documented reason for the delay and no new scheduled completion date.

In addition, the CPSC does not consistently meet the established remediation dates noted in the agency's automated certification and accreditation tool (CSAM) or adequately track and document the updates to the remediation efforts. While it was determined that quantitative metrics obtained via CSAM for the recorded

POA&Ms are distributed monthly, the CPSC was unable to provide evidence of an adequate qualitative analysis of all relevant information. For example, the weakness status for 24 weaknesses due for completion in 2017 is “not started” when it should be delayed. This is an indication of a lack of a qualitative review of the POA&Ms.

Criteria

NIST SP 800-53, Rev 4 requires the development of POA&Ms for the information system to document the organization’s planned actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

OMB Memorandum 14-04 states that while “agencies are no longer required to follow the exact format prescribed in the POA&M examples in OMB Memorandum 04-25, they must still include all of the associated data elements in their POA&Ms.” OMB Memorandum 04-25 requires the following eight data elements: severity and brief description of the weakness, identity of the office or organization that the agency head will hold responsible for resolving the weakness, estimated funding resources required to resolve the weakness, scheduled completion date for resolving the weakness, key milestones with completion dates, changes to milestones, source of the weakness, and status.

Cause

Management has not dedicated the resources required to adequately document and remediate POA&Ms in a timely manner or to perform analytics on the monthly report derived from CSAM.

Effect

The lack of documentation to support the POA&Ms increases the risk of unnecessarily prolonged weaknesses or deficiencies within the information system or processes supporting the information systems.

Recommendation

We recommend management:

44. Establish and implement policies and procedures that require the documentation of POA&Ms with the OMB-required level of granularity.
45. Establish appropriate dates to remediate issues reported and documented as part of the POA&M process.
46. Track all changes to POA&M milestones and milestone dates.
47. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

5.17 FINDING 17: INADEQUATE INCIDENT RESPONSE CAPABILITIES

Condition

The CPSC does not utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Also, the CPSC does not document the incident response process adequately enough to evidence that incidents are remediated in a timely manner.

Criteria

NIST 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Additionally, NIST requires the incident response activities to be coordinated with contingency planning activities and incorporated into lessons learned from ongoing incident handling activities.

Cause

Management has not dedicated the resources required to implement the profiling techniques necessary to baseline network operations and the characteristics of expected data flows for users and systems or to ensure the proper tracking of timely resolution of incidents.

Effect

Not implementing adequate profiling techniques for expected activities may increase the likelihood of a non-detected breach. Additionally, not remediating incidents timely can prevent the CPSC from minimizing damage to its information security.

Recommendation

We recommend management:

51. Identify and implement appropriate profiling techniques to baseline network operations and the characteristics of expected data flows for users and systems.

[redacted]

6. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 6-1: Index of Recommendations

Finding	Recommendation
Finding #1	1. Obtain completed annual A&A packages with valid ATO for all of the CPSC's major systems.
Finding #2	2. [redacted]
Finding #3	3. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance.
	4. Develop, document, and implement a process to classify agency systems as "major" or "minor" in accordance with OMB Circular A-130.
	5. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications.
	6. [redacted]
	7. Define and document the taxonomy of the CPSC's systems to be classified as one of the following types: IT system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC's operational mission, facility, or Social Media) in accordance with FEA.
	8. [redacted]
Finding #4	9. [redacted]
	10. [redacted]
	11. Define and implement identification and authentication policies and procedures.
	12. Automatically revoke temporary and emergency access after a specified period of time.
Finding #5	13. Define and document a strategy (which include specific milestones) to implement FICAM.
	14. Integrate ICAM strategy and activities into the enterprise architecture and ISCM.
Finding #6	15. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security and privacy (e.g., Executive Risk Council) are required to participate in role-

Finding	Recommendation
	based and/or specialized training. 16. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities. 17. Develop/tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals.
Finding #7	18. Perform a gap analysis to identify all NIST SP 800-53, Rev 4 security controls that were not documented and assessed. 19. Document the implementation of all relevant security controls identified in the gap analysis. 20. Assess the implementation of all relevant security controls that were identified in the gap analysis. 21. Update the implementation statements for the program management family of controls in the GSS LAN's SSP to facilitate an assessment of the effectiveness of those controls. 22. Update the GSS LAN SSP to clearly indicate which controls are common controls, and who is responsible for their implementation. 23. Update the CPSC ISCM Plan to specify the assessment frequency, monitoring frequency, and annual assessment testing schedule for the program management family of security controls, and the privacy controls.
Finding #8	24. Develop an EA to be integrated into the Risk Management Process.
Finding #9	25. Develop and enforce a CM plan to that ensures it includes all requisite information. 26. Develop and implement a set of CM procedures in accordance with the inherited CM Policy which includes appropriate measures for all hardware, software, and supporting infrastructure (e.g., equipment, networks, and operating systems). 27. [redacted] 28. Further define the resource designations for a Change Control Board. 29. Identify and document the characteristics of items that are to be placed under CM control. 30. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of changes. 31. [redacted]

Finding	Recommendation
	32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service.
Finding #10	33. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (e.g., NIST SP 800-34/53, FCD1, NIST CSF, and NARA guidance). 34. Develop, document, and distribute all required Contingency Planning documents (e.g., organization-wide COOP and BIA, Disaster Recovery Plan, BCPs, and ISCPs) in accordance with appropriate federal and best practice guidance. 35. Test the set of documented contingency plans. 36. Integrate documented contingency plans with the other relevant agency planning areas.
Finding #11	37. Develop, document, and distribute all required procedures for the destruction or reuse of media containing PII or other sensitive agency data (e.g., proprietary information). 38. [redacted] 39.
Finding #12	40. Establish and implement policies and procedures to require coordination between EXIT and procurement to facilitate identification and incorporation of the appropriate contract clauses within all contracts.
Finding #13	41. Develop and implement an ERM program based on NIST guidance and guidance from the ERM Playbook (A-123, Section II requirement). This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC. 42. Identify, document, and implement a strategy to determine the organizational risk tolerance and adequately document the approach in the Risk Management Strategy, policies, and procedures. 43. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.
Finding #14	44. Establish and implement policies and procedures that require the documentation of POA&Ms with the OMB-required level of granularity. 45. Establish appropriate dates to remediate issues reported and documented as part of the POA&M process. 46. Track all changes to POA&M milestones and milestone

Finding	Recommendation
	dates. 47. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.
Finding #15	48. [redacted]
Finding #16	49. 50. [redacted]
Finding #17	51. Identify and implement appropriate profiling techniques to baseline network operations and the characteristics of expected data flows for users and systems. 52. [redacted]

Appendix A. Objective, Scope, and Methodology

A.1 Objective

The objective was to perform an independent evaluation of the CPSC's implementation of FISMA for FY 2018. In support of this objective, Carson conducted a high-level, qualitative review in accordance with OMB Memorandum 18-02, *Fiscal Year 2017 - 2018 Guidance on Federal Information Security and Privacy Management Requirements*, reporting guidelines.

A.2 Scope

The evaluation focused on reviewing the CPSC's implementation of FISMA for FY 2018. The evaluation included an assessment of the effectiveness of the CPSC's information security policies, procedures, and practices; and a review of information security policies, procedures, and practices of a representative subset of the CPSC's information systems, including contractor systems and systems provided by other federal agencies. Five major CPSC systems were selected for evaluation:

- GSS LAN
- Consumer Product Safety Risk Management System
- CPSC Public Website (CPSC.gov)
- Dynamic Case Management
- International Trade Data System/Risk Automation Methodology System

The evaluation was conducted at the CPSC's headquarters from July 2018 through September 2018. Any information received from the CPSC subsequent to the completion of fieldwork was incorporated when possible.

From a program management perspective, the assessment was tracked by eight (8) specific tasks:

- Task 1: Initial Meeting
- Task 2: Independence Statement/Quality Control Assessment Statement
- Task 3: Staff List and Competency Evidence
- Task 4: Entrance and Exit Conferences
- Task 5: Project Management Plan
- Task 6: Monthly Meetings
- Task 7: Draft Report and Response for Cyber Scope/Draft FISMA Report
- Task 8: Final FISMA Report

A.3 Methodology

Carson performed qualitative analyses to assess the effectiveness of the CPSC's efforts to secure its information systems. The evaluation included an assessment of the NIST Cybersecurity Framework Function Levels, as specified in the FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics:

- Identify (Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- Protect (Date Protection and Privacy)
- Protect (Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident Response)
- Recover (Contingency Planning)

Evaluation, testing, and analysis were performed in accordance with guidance from the following:

- Chief Financial Officers Council, *Enterprise Risk Management Playbook*
- CIO Council/Chief Acquisition Officer Council, *Cloud Computing Contract Best Practices*
- Council of Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*
- Cybersecurity Sprint
- Cybersecurity Strategy and Implementation Plan
- Department of Homeland Security Binding Operational Directive 15-01
- Department of Homeland Security Binding Operational Directive 17-01
- Department of Homeland Security Cyber Incident Reporting Unified Message
- E-Government Act of 2002
- Federal Acquisition Regulation sections 39.101, 105, 52.224-1, 52.224-2, and 52.239-1
- Federal Continuity Directive 1
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture Framework
- Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance
- Federal Information Processing Standards 199
- Federal Information Processing Standards 201-2
- Federal Information Security Modernization Act of 2014
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- FY 2018 Chief Information Officer Federal Information Security Modernization Act of 2014 Metrics
- FY 2018 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Metrics
- Homeland Security Presidential Directive 12
- Government Accountability Office, *Standards for Internal Control in the Federal Government*

- National Archives and Records Administration, *Guidance on Information Systems Security Records*
- National Cybersecurity Workforce Framework
- National Insider Threat Policy
- National Institute of Standards and Technology Cybersecurity Framework
- National Institute of Standards and Technology (NIST) SP 800-44
- National Institute of Standards and Technology (NIST) SP 800-122
- National Institute of Standards and Technology (NIST) SP 800- 50
- National Institute of Standards and Technology (NIST) SP 800-181
- National Institute of Standards and Technology (NIST) SP 800-184
- National Institute of Standards and Technology (NIST) SP 800-128
- National Institute of Standards and Technology (NIST) SP 800-161
- National Institute of Standards and Technology (NIST) SP 800-181 (Draft)
- National Institute of Standards and Technology (NIST) SP 800-30
- National Institute of Standards and Technology (NIST) SP 800-34
- National Institute of Standards and Technology (NIST) SP 800-37, Rev 1
- National Institute of Standards and Technology (NIST) SP 800-39
- National Institute of Standards and Technology (NIST) SP 800-40, Rev 3
- National Institute of Standards and Technology (NIST) SP 800-53, Rev 4
- National Institute of Standards and Technology (NIST) SP 800-60
- National Institute of Standards and Technology (NIST) SP 800-61, Rev 2
- National Institute of Standards and Technology (NIST) SP 800-63
- National Institute of Standards and Technology (NIST) SP 800-83
- National Institute of Standards and Technology (NIST) SP 800-84
- National Institute of Standards and Technology (NIST) SP 800-86
- National Institute of Standards and Technology (NIST) SP 800-137
- National Institute of Standards and Technology (NIST) Supplemental Guidance on Ongoing Authorization
- Office of Management and Budget Circular No. A-123
- Office of Management and Budget Circular No. A-130, Appendix I
- Office of Management and Budget Circular No. A-11
- Office of Management and Budget, Memorandum 04-25
- Office of Management and Budget, Memorandum 08-05
- Office of Management and Budget, Memorandum 14-03
- Office of Management and Budget, Memorandum 14-04
- Office of Management and Budget, Memorandum 16-03
- Office of Management and Budget, Memorandum 16-04
- Office of Management and Budget, Memorandum 16-17
- Office of Management and Budget, Memorandum 17-09
- Office of Management and Budget, Memorandum 17-12
- Office of Management and Budget, Memorandum 17-25
- Office of Management and Budget, Memorandum 18-02
- Presidential Policy Directive - 41
- President's Management Council

- Privacy Act of 1974
- SANS Institute Critical Security Controls
- Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- US-Computer Emergency Readiness Team - *Federal Incident Notification & Response Guidelines*
- US-Computer Emergency Readiness Team - *Incident Notification Guidelines*
- US-Computer Emergency Readiness Team - *Incident Response Guidelines*

Appendix B. Management Views on Conclusions and Findings

Finding 1: Lack of completed Assessment and Authorization (A&A) packages for major systems with signed Authority to Operate (ATO)

Management concurs with this finding.

Consistent with our approaches for the past 2 years management planned for and scheduled the Department of Transportation's Federal ISSLOB program to conduct the FY 2018 independent security assessment activities. In April, as the agency was actively coordinating with the Department of Transportation service provider and within a week of our target start date for beginning the assessment, we were notified that they would be unable to perform the assessment as had been planned in FY 2017 this year due to an unexpected loss of staff.

Management immediately began seeking alternative providers to support this requirement and ultimately entered into a new agreement with the Department of the Interior to provide these services. The short notice provided by the Department of Transportation, coupled with the need to identify an alternative service provider willing to perform the assessment and finalize the interagency contract commitments, created unavoidable delays that caused the required independent assessment results to not be available to support required updates to Assessment and Authorization packages.

Management communicated the loss of our planned independent assessment service provider and the potential impact during the FISMA audit entrance conference with our Inspector General. Management is committed to completing this task as expeditiously as possible and is projecting completion of all security assessment & authorization activities—including Authorizations to Operate (ATO) by 10/31/2018.

Finding 2: Lack of enforcement of Personal Identity Verification (PIV) across the organization

Management concurs with this finding.

[redacted]

[redacted]

[redacted]

[redacted]

<u>Finding 3: Inadequate implementation of an information system inventory and an information system component (asset) inventory</u>

Management concurs with this finding.

Current practices are substantially effective. Management currently has manual processes in place to manage software licenses. Automated license management is not mandated; however, CPSC is actively investigating approaches for automating our software asset management processes.

In accordance with NIST SP 800-18, all agency information systems are covered by a system security plan and identified as a major application or general support system. The agency's current practice for classifying information systems as "major" includes an assessment of the information that a system contains, processes, stores, or transmits—or because of the system's criticality to the agency's mission.

Specific system security plans for minor applications are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate. Management has included in its GSS LAN security plan a list of all agency applications that inherit controls from the GSS LAN.

Agency information systems and the information resident within these systems are categorized based on a FIPS 199 impact analysis. Then a determination is made as to which systems in the inventory can be logically grouped into major applications or general support systems. The FIPS 199 impact levels are considered when the system boundaries are drawn and when selecting the initial set of security controls.

The property management system is listed as a "minor" application within the GSS LAN's System Security Plan—as it inherits the overwhelming majority of its security controls from the GSS LAN. Reclassifying property management as a "major information system" would introduce increased management costs that would exceed current losses of property—with no corresponding increase in security. This condition would not comply with requirements in OMB M-16-17, which requires that the benefit of controls outweigh the costs.

[redacted]

[redacted]

<u>Finding 4: Lack of Enforcement around the Principle of Least Privilege and/or Separation of Duties for Privileged Accounts</u>

Management concurs with this finding.

CPSC has a current and conforming Identification and Authentication policy. CPSC intends to review associated procedures to confirm alignment with policy and identify potential gaps.

[redacted]

[redacted]

[redacted]

Finding 5: Lack of Defined Strategy and Milestones to Align with Federated Identity, Credential, and Access Management (FICAM) and Implementation of DHS's CDM Program

Management concurs with this finding.

CPSC performs identity, credential and access management functions but has not incorporated the FICAM architecture guidance into the review of these functions. Identity and credential management processes, data, and systems architecture elements are largely provided through shared service providers for HR and PIV credential management. It is not clear that risk would be substantially reduced through a redundant CPSC driven review of those architectural designs. Management is aware of, and actively working to resolve several areas in need of improvement relative to access management.

Management will review the FICAM guidance and evaluate how it may be applied to potential related process improvements with a primary focus on access management, currently considered to be the area of greatest risk.

[redacted]

Finding 6: Role-Based Training Requirements around Security and Privacy are not Adequately Defined across the Organization

Management concurs with this finding.

Current practices are substantially effective. 100% of users with network access completed mandatory security, privacy, and records management 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, firewall administration, or management oversight of these programs, including the CISO and CIO, are considered to have significant security responsibilities and receive the appropriate role-based training.*

Management will consult with the agency's training coordinator to help define additional agency roles with significant security responsibilities – and therefore require additional security training.

Finding 7: Lack of Defined and Communicated Security Control Implementation and ISCM Activities

Management concurs with this finding.

Management maintains that it followed NIST guidance in the assessment of agency information systems and provided evidence of the assessment of privacy controls.

Management intends to update the ISCM plan to include assessment and monitoring frequencies for both the program management and privacy controls.

Management will review the GSS LAN system security plan and ensure that program management implementation statements are properly parameterized—where required.

Management will also review security plans to determine if control classification and responsible party can be added.

Finding 8: No Existing Enterprise Architecture Documented for Managing Risk

Management concurs with this finding.

The EA implementation approach focusing on relating agency data to systems and mission functions will expedite the value of the EA program in regard to risk management, overall information protection, and practical utility to the agency mission.

Management concurs that development and implementation of a comprehensive EA program will require sustained effort and intends to continue progress. Management's efforts in regard to EA development will continue to factor in benefits to agency information security.

Finding 9: Insufficient Documentation around Configuration Management

Management concurs with this finding.

EXIT has significantly increased the rigor of its configuration management processes to include formal review by key functional personnel (including security) prior to approval for implementation. This has *resulted in better coordination and fewer unanticipated system conflicts as well as better conformance to security policy requirements. Management developed Configuration Management plans for all of its major systems in FY17 but acknowledges there are still activities that need to be completed for full implementation.*

[redacted]

Finding 10: Lack of Formally Documented Contingency Plans

Management concurs with this finding.

Management has not completed testing of all individual contingency plans but plans to complete this activity in FY19.

Management completed development of individual contingency plans (ISCPs) for all major systems in FY 2017. Management reviewed and re-authorized the plans in FY 2018.

Management completed individual Business Impact Assessments (BIA) for each major system in FY 2017. Management plans to develop an organizational BIA in FY 2019 using input from the individual BIAs.

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.

Finding 11: Media Sanitization Prior to Disposal

Management concurs with this finding.

Management will document media sanitization processes.

Management maintains an inventory of PII by information system and has established related policies as appropriate for the protection of PII collected, used, maintained, and shared by information systems. However, roles and responsibilities for the effective implementation of PII protection policies have not been fully defined.

Finding 12: Contract Language Does Not Adequately Identify Requirements to Mitigate Risks

Management concurs with this finding.

EXIT and the Office of Procurement have coordinated closely on updating contract clauses. Management will, however, review the referenced areas in the finding to incorporate missing clauses into standard formats to the extent possible. Management has in place internal operating procedures for procurement covering the specified FAR references identified in the description of this finding.

The finding references a lack of processes to affirm security controls provided by third parties. Management believes those requirements are covered by current policies and system specific requirements contained within ISAs with third party governmental service providers and assessments of contracted systems.

Finding 13: Risk from an Organizational Level is Not Adequately Managed

Management concurs with this finding.

In FY 2017, Management developed an IT-based risk management strategy that defines and documents organizational approaches for assessing, evaluating, and responding to risk; risk tolerance; and monitoring risk for agency systems. However, determining organizational risk tolerance is a Tier 1 enterprise-level activity beyond the scope of IT risk management activities. Progress is anticipated as part of the CPSC Risk Management Council and employed as part of the Enterprise Risk Management Implementation Plan.

In FY 2018 CPSC integrated the Cybersecurity Critical Infrastructure Framework with the CPSC Enterprise Risk Management Profile by updating the information related profile elements to explicitly reflect the risk areas. This not only aligns the two risk perspectives but also allows for detailed control visibility associated with these elements.

Finding 14: Plan of Actions and Milestones (POA&Ms) Are Not Adequately Documented and Implemented

Management concurs with this finding.

Management believes that its POAM review process is substantially effective while recognizing that some data elements not critical for implementation may not be completed in all cases. POAM resolution is prioritized by risk evaluations and available resources for resolution.

Management will review the POAM listing and address missing dates as recommended. The items missing dates predate existing policy but were not updated.

Management provides systems owners and authorizing official with a monthly report of POAM status, completion percentages, numbers of resolved POAMs, etc. Management believes that analytics provided in monthly reports meet agency and governmental policy requirements.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

<u>Finding 17: Inadequate Incident Response Capabilities</u>

Management concurs with this finding.

Management will review available tools and techniques to identify a cost-effective method to implement profiling techniques across agency information systems.

Management believes it current practices related to tracking and the resolution of incidents is substantially effective. Management currently utilizes an electronic system to track all reported incidents. Key information about each incident—including incident type, incident number, incident status, incident start date, incident detected date, incident description, and incident closed date—is recorded and managed by security analysts. Management will review its incident response plan and will define and implement processes to ensure the timely resolution of incidents.

Appendix C. Acronyms

A&A	Assessment and Authorization
ATO	Authorization To Operate
BCP	Business Continuity Plan
BIA	Business Impact Assessment
Carson	Richard S. Carson & Associates, Inc.
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CFR	U.S. Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
CONOPS	Concept of Operations
COOP	Continuity of Operation Plan
CPSC	U.S. Consumer Product Safety Commission
CPSIA	Consumer Product Safety Improvement Act
CSAM	Cybersecurity Assessment and Management
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
EA	Enterprise Architecture
ERM	Enterprise Risk Management
EXIT	Office of Information and Technology Services
FAR	Federal Acquisition Regulations
FCD1	Federal Continuity Directive 1
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Modernization Act of 2014
FMPS	Division of Procurement Services
FY	Fiscal Year
GSS LAN	General Support System Local Area Network
HSPD-12	Homeland Security Presidential Directive 12
IA	Identification and Authentication
ICAM	Identity, Credential, and Access Management
ISCM	Information System Continuous Monitoring
ISCP	Information System Security Plan
IT	Information Technology
NAC	Network Access Control
NARA	National Archive and Records Administration

NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PM	Program Management
POA&Ms	Plan of Actions and Milestones
Rev	Revision
SA	Security Assessment
SDLC	System Development Lifecycle
SP	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connections

Contact Us

If you want to confidentially report or discuss any instance of misconduct, fraud, waste, abuse, or mismanagement involving CPSC’s programs and operations, please contact the CPSC Office of Inspector General.

Call:

Inspector General's HOTLINE: 301-504-7906
Or: 1-866-230-6229

Click here for complaint form.

Click here for CPSC OIG website.

Or Write:

Office of Inspector General
Consumer Product Safety Commission
4330 East-West Highway, Room 702
Bethesda MD 20814