Office of Inspector General

U.S. Consumer Product Safety Commission

Evaluation of CPSC's FISMA Implementation for FY 2019

October 30, 2019

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 Office of Inspector General.

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 30, 2019

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

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Evaluation of CPSC's FISMA Implementation for FY 2019

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 2019, 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 18 findings and 55 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, including 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 CPSC's implementation of FISMA for Fiscal Year (FY) 2019. This report serves to document CPSC's compliance with the requirements of FISMA. In evaluating CPSC's progress in implementing its agency-wide information security program, we specifically assessed 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. CPSC has continued to focus its efforts on the implementation of the following processes/systems:

- Automation of privileged access management for elevated network access.
- Development of a formal Enterprise Architecture (EA)
- Engagement with stakeholders in support of the establishment of an Executive Risk function
- Rollout of a role-based training program
- Information Security Continuous Monitoring (ISCM) program
- Documenting and enforcing protocols controlling the destruction/reuse of media containing Personally Identifiable Information (PII) or other sensitive agency data (e.g., proprietary information)
- Enforcement of Personal Identification Verification (PIV) authentication.

- Utilization of Simple Mail Transfer Protocol (SMTP) Domain-based Message Authentication, Reporting and Conformance (DMARC) checks
- Enhanced network defense support
- Participation in DHS's EINSTEIN 3 Accelerated program.

We noted eighteen (18) findings in this year's FISMA review. The Information Technology (IT) challenges currently facing 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 CPSC's implementation of FISMA, we make 55 recommendations to enhance IT Security.

1. OBJECTIVE

The objective was to perform an independent evaluation of CPSC's implementation of FISMA for FY 2019.

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, including 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 (M) 19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 25, 2018, requires the OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via CyberScope.

CPSC OIG retained Carson to perform an independent evaluation of CPSC's implementation of FISMA for FY 2019. This report presents the results of that independent evaluation. Carson will also prepare responses to OMB's annual FISMA reporting questions for OIGs, and 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 CPSC's FY 2019 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 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 CPSC's decision to not dedicate the resources necessary to support the implementation of planned activities.

5. FINDINGS

5.1 FINDING 1: INADEQUATE INFORMATION SYSTEMS INVENTORY

Condition

CPSC uses the Cyber Security Assessment and Management System (CSAM) to monitor the authorization status of their inventory of information systems and to track interconnection security agreements. The CPSC inventory of systems comprises one general support system (GSS) and four major applications. In addition, over 70 "minor" applications are supported by the GSS. These minor applications include both in-house applications, third party applications, and cloud-hosted applications.

The CPSC ISCM Plan describes the strategy for continuously monitoring the security control effectiveness of the GSS and four major applications. The CPSC Interconnection and Contractor Oversight Policy describes procedures for ongoing monitoring of security control compliance by external service providers, including cloud service providers.

However, CPSC does not have a process for developing and maintaining a comprehensive and accurate inventory of its information systems. The implementation statement for control Program Management (PM)-05, Information System Inventory, in the system security plan for the GSS does not describe how CPSC develops and maintains an inventory of information systems. Rather, it describes methods for maintaining inventories of information system components (e.g., desktops, laptops, servers, etc.). The CPSC inventory of information systems included in the GSS system security plan does not indicate which minor applications are third party applications and which are cloud-hosted applications. In addition, CPSC does not require the authorization of third party and cloud systems (e.g., Authorization to Use), and CPSC does not require continuous monitoring of these systems.

Criteria

FISMA requires agencies to develop and maintain an inventory of information systems operated by or under control of the agency. In addition, the inventory should include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

OMB Circular A-130, *Managing Information as a Strategic Resource*, requires agencies to provide oversight of information systems used or operated by contractors or other entities on behalf of the federal government or that collect or maintain federal information on behalf of the federal government (i.e., third party/contractor operated systems). This oversight includes ensuring such systems are included in the agency's inventory of information systems.

OMB requires agencies to report annually on the security categorization and authorization status of their inventory of information systems, including their inventory of contractor-operated systems. OMB also requires agencies to report on the types of cloud services used by the agency and the authorization status of those cloud offerings.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires organizations to do the following:

- develop and maintain an inventory of its information systems
- authorize connections from the information system to other information systems through the use of Interconnection Security Agreements
- implement a continuous monitoring program to facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions

Cause

CPSC has not dedicated the resources necessary to fully document and maintain an information systems inventory.

Effect

Without a comprehensive information system inventory, CPSC cannot effectively implement a continuous monitoring program in accordance with their ISCM Plan and the Interconnection and Contractor Oversight Policy which could lead to increased risk to CPSC's information and information system confidentiality, integrity, and availability.

Recommendation

We recommend management:

1. Update the GSS system security plan compliance description for all NIST security controls and describe CPSC's process for developing and maintaining a comprehensive and accurate inventory of information systems.
2. Update the inventory of minor applications in the GSS system security plan to indicate which applications are in-house, third party, or cloud-hosted.

5.2 FINDING 2: PIV NOT ADEQUATELY ENFORCED

Condition

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

[redacted]

Criteria

OMB M11-11 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 OMB on October 30, 2015, requires that federal agencies use PIV credentials for authenticating privileged user accounts.

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

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

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

3. [redacted]

5.3 FINDING 3: INADEQUATE INFORMATION SYSTEM COMPONENT INVENTORY

Condition

CPSC has implemented various tools to develop an 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, CPSC has not compiled and leveraged a comprehensive inventory of hardware and software to achieve effective information system component accountability, or addressed the following areas:

- [redacted]

Criteria

NIST SP 800-53 requires organizations to develop and maintain an inventory of all components within the authorization boundary of each information system 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*, and NIST SP 800-37, Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Appendix G, further outlines requirements for the security-related information pertaining to a system component inventory and additional considerations for determining authorization boundaries.

Cause

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 complete these tasks.

Effect

The effect of not having accurate and up-to-date hardware, software, and system component inventories is that the CPSC does not have a full understanding of their system environment or the risks associated with that environment. [redacted]

Recommendation

We recommend management:

4. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance.
5. Establish and implement a policy and procedures to manage software licenses using automated monitoring and expiration notifications.

[redacted]

7. Define and document the taxonomy of CPSC's information system components, and classify each information system component as, at minimum, one of the following types: IT system (e.g., proprietary and/or owned by 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 CPSC's operational mission, facility, or social media).

[redacted]

5.4 FINDING 4: INADEQUATE IMPLEMENTATION OF PRIVILEGED USER CONTROLS

Condition

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

- [redacted]

- [redacted]

Criteria

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

- [redacted]

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

[redacted]

[redacted]

13. Define and implement the identification and authentication policies and procedures.

[redacted]

5.5 FINDING 5: INCOMPLETE FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) ROADMAP

Condition

The CPSC Access Management Plan requires CPSC employees and contractors to utilize PIV cards to access agency resources. [redacted] However, the CPSC was unable to provide a strategy with milestones which supports the implementation of FICAM segment architecture and phase two of the DHS's Continuous Diagnostics and Mitigation (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:

15. Define and document a strategy (including specific milestones) to implement FICAM.
16. Integrate ICAM strategy and activities into the EA and ISCM.

5.6 FINDING 6: INEFFECTIVE ROLE-BASED TRAINING REQUIREMENTS

Condition

The CPSC Awareness and Training Policy outlines requirements for EXIT staff, and CPSC has fully implemented this policy. In addition, CPSC's electronic training solution maintains training records for all CPSC personnel. However, the policy does not require all specified CPSC staff to complete role-based training, and role-based training is not provided to these individuals. Based on requirements outlined in 5 Code of Federal Regulation (CFR) 930.301, role-based training must be provided to all personnel that affect security. This includes members of the Risk Executive Function and all other applicable roles described in the CFR. Additionally, this policy does not adequately address role-based training for personnel with specialized privacy responsibilities in accordance with federal requirements and the NIST SP 800-53, Accountability, Audit, and Risk Management (AR)-5 guidance. The agency-specific policies, procedures, and responsibilities were not defined within the security awareness or role-based trainings provided by management. Additionally, 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 CPSC's organization, requirements, types of systems, culture, mission, and risk environment.

Criteria

NIST SP 800-53 requires the development and dissemination of a security awareness and training policy and supporting procedures. These policies and procedures should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

NIST SP 800-53 also prescribes specific roles which must receive specialized security training. These roles which must receive specialized security training include: enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software. Additionally, individuals that carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs must also receive specialized training.

Moreover, as codified in 5 CFR 930.301 all personnel in roles which affect security must be provided role-based security training. These roles include: executives,

program and functional managers, Chief Information Officers (CIO), 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.

Cause

Management has not made the development and dissemination of role-based training for all affected staff a priority.

Effect

Staff are inadequately trained in security and privacy requirements. This inadequate training increases the risk of the improper implementation of agency-defined policies and procedures which can lead to data breaches and other security incidents.

Recommendation

We recommend management:

17. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training.
18. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities.
19. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals.

5.7 FINDING 7: INADEQUATE ISCM PROGRAM

Condition

CPSC has defined processes for performing security control assessments, system authorizations, and continuous monitoring of security controls. CPSC utilizes the GSS Local Area Network (GSS LAN) System Security Plan (SSP) as its organization-wide information security program plan. CPSC also established an ISCM Plan which defines the assessment frequency, ranging from 1 year to 5 years, for each security control along with a schedule for performing annual system assessments through FY 2020. In addition, the CPSC ISCM plan defines the security control monitoring

frequencies (e.g., monthly, quarterly, semi-annually, and annually). However, CPSC has not documented or assessed the implementation of all relevant security controls associated with all agency information systems.

The FY 2018 FISMA independent evaluation found that CPSC had not conducted a security assessment of the privacy controls specified in NIST SP 800-53, Appendix J. In FY 2019, CPSC evaluated some, but not all, of the privacy controls specified in NIST SP 800-53, Appendix J. Specifically, controls AR-07, AR-08, Data Quality and Integrity (DI)-01, DI-02, and Individual Participation and Redress (IP)-01 through IP-04 were not evaluated. In addition, the FY 2019 GSS LAN SSP does not include these privacy controls nor does it include the justification (i.e., scoping/tailoring guidance) for excluding these controls. Please note, all tailoring activities should be documented in the system security plan and as privacy controls are independent of any security control baseline, they should be implemented and evaluated at the organizational level.

The FY 2018 FISMA independent evaluation also found that the CPSC GSS LAN SSP included references to the PM controls required by NIST SP 800-53; however, they were not adequately documented. The implementation statements included in this SSP were not all properly parameterized or sufficient to facilitate an assessment of the effectiveness of these controls. In the FY 2019 CPSC GSS LAN SSP, the implementation statements for the PM controls included only minor grammatical changes. In addition, five PM controls were removed from the FY 2019 CPSC GSS LAN SSP. All tailoring activities should be documented in the system security plan; however, there is no indication as to why these five controls were removed.

In addition, the FY 2018 FISMA independent evaluation found that security controls descriptions in the CPSC GSS LAN SSP did not include any indication of which controls are common controls or who is responsible for the implementation of these common controls. A table was added at the end of the FY 2019 CPSC GSS LAN SSP that indicates which controls are provided by the GSS LAN to the subordinate systems and which controls are hybrid controls. However, this table is missing the privacy controls, and does not indicate the individual responsible for implementing the common controls.

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 a third party.

The information security PM family of controls are described in NIST SP 800-53, Appendix G. These controls should be implemented at the organizational level (i.e., common controls). NIST SP 800-53, Appendix J, describes privacy controls, which are also implemented at the organizational level, based on the privacy requirements of the organization and the need to protect the personally identifiable information collected and maintained by CPSC information systems and programs. Unlike the controls found in the security control catalog in NIST SP 800-53, Appendix F, the PM and privacy controls are all entity-level controls independent of any security control baseline.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, describes the process for scoping/tailoring baseline security controls which includes specifying agency-defined parameters. Scoping guidance also includes identification of common controls, as well as controls that are not applicable in a particular system or environment. Per NIST SP 800-18, all tailoring activities should be documented in the system security plan. For example, common controls should be documented and the individual responsible for implementing the common controls should be listed in the security plan. Descriptions of security controls in a security plan should include:

- the security control title
- how the security control is being implemented or planned to be implemented any scoping/tailoring performed to the security controls and justification for this scoping/tailoring
- 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. These guidelines include requirements and recommendations for conducting 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 perform assessments of all required security controls.

Effect

The lack of an adequately implemented ISCM program limits management awareness of the information security risks associated with agency information and information systems.

Recommendation

We recommend management:

20. Perform a gap analysis to identify all NIST SP 800-53 privacy controls from NIST SP 800-53, Appendix J that were not documented and assessed.
21. Document the implementation of all relevant privacy controls identified in the gap analysis in appropriate the system security plans.
22. Assess the implementation of all relevant privacy controls that were identified in the gap analysis.
23. Update the implementation statements for the PM family of controls in the GSS LAN's SSP to facilitate an assessment of the effectiveness of those controls.
24. Update the GSS LAN SSP to clearly indicate which controls are common controls and who is responsible for their implementation.

5.8 FINDING 8: NO EXISTING EA

Condition

Although CPSC has documented a risk management approach, CPSC has not defined an EA and integrated that EA into the agency's risk management approach; 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 requires federal organizations to:

- develop an information security architecture
- review and update the information security architecture in accordance with the EA
- ensure planned information security architecture changes are appropriately aligned with security plans, Concept of Operations (or better known as CONOPS), and organizational procurements/acquisitions
- employ security considerations throughout system development life cycle (SDLC)
- define and document information security roles and responsibilities throughout the SDLC
- identify positions 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

The Federal Enterprise Architecture (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 CPSC's mission success.

Recommendation

We recommend management:

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

5.9 FINDING 9: INEFFECTIVE CONFIGURATION MANAGEMENT

Condition

CPSC has developed a GSS Configuration Management (CM) policy and has documented a CM procedure to support the CM policy. However, management has not fully implemented the CM policies and procedures.

Also, no organizational-specific CM plan has been established and implemented to support the policy. As such, CPSC has not documented a process for identifying and integrating configuration items throughout the system development life cycle.

[redacted]

[redacted]

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

Criteria

NIST SP 800-53 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 to agency management on how to properly and securely implement CM.

NIST established the Cybersecurity Framework (CSF) in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The CSF was established, in part, to foster risk and cybersecurity management communications. The CSF is mapped to NIST SP 800-53 and to the Center for Internet Security (CIS) Top 20 Critical Security Controls. [redacted]

Cause

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

Effect

Without a fully developed, documented, and communicated set of comprehensive CM policies and procedures, CPSC risks not maintaining the confidentiality, integrity and availability of assets supporting its mission.

Recommendation

We recommend management:

26. Develop and implement a CM plan to ensure it includes all requisite information.

[redacted]

29. Further define the resource designations for a Change Control Board.
30. Identify and document the characteristics of items that are to be placed under CM control.
31. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations.
32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program.

5.10 FINDING 10: LACK OF FORMALLY DOCUMENTED CONTINGENCY PLANS

Condition

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, and Business Continuity Plans (BCPs), and Information System Contingency Plans (ISCPs). Based on this lack of documentation, it was determined that CPSC has not documented or assessed the contingency steps required to recover agency systems and processes to support 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

While, CPSC has completed BIAs for existing major systems, it has not completed or distributed an organizational BIA. Additionally, supporting Standard Operating Procedures (SOPs) for the major systems have not been developed and distributed.

Criteria

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

Additionally, NIST SP 800-34, Revision 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.

CSF 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 (5) functions listed above.

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 schedule for protecting security of information technology systems and data, and responding to computer security incidents.

Cause

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

Effect
Without a developed, documented, and communicated set of contingency plans and processes, CPSC risks not being able to recover agency systems and processes to support 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 (ex. NIST SP 800-34/53, FCD1, NIST CSF, and NARA guidance).
34. Develop, document, and distribute all required Contingency Planning documents (ex. 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: INADEQUATE MEDIA SANITIZATION PROCEDURES

Condition
CPSC has established protocols to sanitize information system media prior to disposal, release out of organizational control, or release for reuse. CPSC utilizes a disk wipe utility to sanitize disk drives, as well as shredders and locked containers to protect data.

[redacted]

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

Cause
[redacted]

Effect

[redacted]

Recommendation

We recommend management:

- [redacted]
- [redacted]

5.12 FINDING 12: INADEQUATE CONTRACT LANGUAGE

Condition

CPSC has developed an SOP that outlines the requirement for agency Contracting Officer Representatives and EXIT to coordinate with the Office of Procurement (FMPS) to ensure the appropriate Federal Acquisition Regulations (FAR) clauses are included in agency contracts for all "incoming requisition procurement packages." But, 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, Security Assessment (SA)-4 or cloud computing requirements are included in agency contracts. Moreover, 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.

CPSC has not updated existing IT contracts 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, SA-4 requirements

Criteria

NIST SP 800-53 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 the 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 introduce and increase the risk of security weaknesses to CPSC arising from the service provider not being contractually required to meet security and privacy requirements.

Recommendation

We recommend management:

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

5.13 FINDING 13: ORGANIZATIONAL LEVEL RISK IS NOT ADEQUATELY MANAGED

Condition

Management has assigned resources to support the development of an organizational risk management plan. However, management's approach does not include a strategy for defining and applying risk tolerance at the organizational level (risk appetite), or calculating and applying risk tolerances at the mission/system level. Therefore, the method to determine the types and severity of risk that management is willing to assume has not been adequately defined.

Moreover, the following activities are not effectively implemented:

- capturing and sharing risk management lessons learned to improve the program
- defining and analyzing qualitative and quantitative performance measures to assess the effectiveness of the risk management strategy
- scenario analysis and modeling of potential responses

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

Lastly, CPSC has not developed a supply chain risk management plan as required by OMB Circular A-130, *Managing Information as a Strategic Resource*.

Criteria

NIST SP 800-53 requires the organization to perform the following:

- 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 provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

The Chief Financial Officer (CFO) Council Enterprise Risk Management 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*.

OMB A-130 requires agencies to consider supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed. Specifically, agencies are required to develop a supply chain risk management plan in order to ensure the integrity, security, resilience, and quality of information systems.

Cause

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

Effect

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

Recommendation

We recommend management:

40. Develop and implement an ERM program based on NIST and ERM Playbook (A-123, Section II requirement) guidance. 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 CPSC.
41. Identify, document, and implement a strategy to determine and define CPSC's risk appetite and tolerances, and apply this approach to prioritizing risk mitigation activities.
42. Develop and implement a supply chain risk management plan.
43. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.

5.14 FINDING 14: INADEQUATE PLAN OF ACTIONS AND MILESTONES (POA&MS) DOCUMENTATION AND IMPLEMENTATION

Condition

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, of the 116 weaknesses in an open status for the June 2019 POA&Ms, 62 have been delayed more than 2 years; however, there is no documented reason for the delay and no new scheduled completion date.

In addition, CPSC does not consistently meet the established remediation dates noted in CSAM or adequately track and document the updates to the remediation efforts. While metrics obtained via CSAM for the recorded POA&Ms are distributed monthly, the CPSC was unable to provide evidence of an adequate qualitative or quantitative analysis of all relevant information.

Criteria

NIST SP 800-53 requires the development of POA&Ms for known information system security weaknesses in order to establish, track, and prioritize the organization's planned remedial actions.

OMB M14-04 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 M04-25 requires the following eight data elements: severity, 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 performed analytics on the monthly report derived from CSAM.

Effect
The lack of analytics increases the likelihood that CPSC is not focusing its efforts on the most serious issues and without documentation to support POA&M dates and status changes there is increased risk that weaknesses or deficiencies within the information system will remain un-remediated longer than is necessary.

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.

5.15 FINDING 15: [redacted]

Condition
[redacted]

- [redacted]

[redacted]

Criteria

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

[redacted]

5.16 FINDING 16: [redacted]

Condition

[redacted]

Criteria

[redacted]

Cause

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

[redacted]

5.17 FINDING 17: INADEQUATE INCIDENT RESPONSE CAPABILITIES

Condition

CPSC has made substantial progress in implementing its incident response capabilities. [redacted] Also, CPSC does not document the incident response process adequately enough to evidence that incidents are remediated in a timely manner.

Criteria

NIST 800-53 requires organizations to implement an incident handling capability for security incidents that includes preparation, detection, 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

[redacted]

Effect

[redacted]

Recommendation

We recommend management:

53. [redacted]
54. Define and implement a process to ensure the timely resolution of incidents. For example, establish routine status reviews for tracking incident response activities to completeness.

5.18 FINDING 18: LACK OF FORMAL PERSONNEL RISK DESIGNATION AND SCREENING PROCEDURES

Condition
CPSC has not established and implemented formal documented policies and procedures through the CPSC D-100 process for assigning position risk designations and performing appropriate screenings.

Criteria
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to assign a risk designation to all organizational positions, establish screening criteria for individuals filling those positions, and review and update position risk designations on a periodic basis. Organizations are also required to screen individuals prior to authorizing access to agency systems, and rescreen individuals on a periodic basis.

Cause
Management has not dedicated the resources required to establish and implement formal processes for assigning position risk designations and performing appropriate screenings.

Effect
Proper position designation is the foundation of an effective and consistent suitability and personnel security program. Failure to consistently assign agency positions at the proper level using established standards may permit individuals access to information they are not properly vetted to access, placing the agency and its data at risk.

Recommendation
We recommend management:

55. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements:

    - performance of periodic reviews of risk designations at least annually
    - explicit position screening criteria for information security role appointments
    - description of how cybersecurity is integrated into human resources practices

6. CONSOLIDATED LIST OF RECOMMENDATIONS

Table 6-1: Index of Recommendations

Finding	Recommendation
Finding #1	1. Update the GSS system security plan compliance description for all NIST security controls and describe CPSC's process for developing and maintaining a comprehensive and accurate inventory of information systems. 2. Update the inventory of minor applications in the GSS system security plan to indicate which applications are in-house, third party, or cloud-hosted.
Finding #2	3. [redacted]
Finding #3	4. Develop, document, and implement a process for determining and defining system boundaries in accordance with NIST guidance. 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 information system components, and classify each information system component as, at minimum, one of the following types: IT system (e.g., proprietary and/or owned by 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 CPSC's operational mission, facility, or social media). 8. [redacted]

Finding	Recommendation
Finding #4	[redacted] 13. Define and implement the identification and authentication policies and procedures. [redacted]
Finding #5	15. Define and document a strategy (including specific milestones) to implement FICAM. 16. Integrate ICAM strategy and activities into the EA and ISCM.
Finding #6	17. Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training. 18. Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities. 19. Develop and tailor security training content for all CPSC personnel with significant security responsibilities, and provide this training to the appropriate individuals.
Finding #7	20. Perform a gap analysis to identify all NIST SP 800-53 privacy controls from NIST SP 800-53, Appendix J that were not documented and assessed. 21. Document the implementation of all relevant privacy controls identified in the gap analysis in appropriate the system security plans. 22. Assess the implementation of all relevant privacy controls that were identified in the gap analysis. 23. Update the implementation statements for the PM family of controls in the GSS LAN's SSP to facilitate an assessment of the effectiveness of those controls. 24. Update the GSS LAN SSP to clearly indicate which controls are common controls and who is responsible for their implementation.

Finding	Recommendation
Finding #8	25. Develop an EA to be integrated into the risk management process.
Finding #9	26. Develop and implement a CM plan to ensure it includes all requisite information. [redacted] 29. Further define the resource designations for a Change Control Board. 30. Identify and document the characteristics of items that are to be placed under CM control. 31. Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations. 32. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program.
Finding #10	33. Develop and document a robust and formal approach to contingency planning for agency systems and processes using the appropriate guidance (ex. 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	[redacted]
Finding #12	39. Establish and implement policies and procedures to require coordination between EXIT and FMPS to facilitate identification and incorporation of the appropriate clauses within all contracts.

Finding	Recommendation
Finding #13	40. Develop and implement an ERM program based on NIST and ERM Playbook (A-123, Section II requirement) guidance. 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 CPSC. 41. Identify, document, and implement a strategy to determine and define CPSC's risk appetite and tolerances, and apply this approach to prioritizing risk mitigation activities. 42. Develop and implement a supply chain risk management plan. 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 dates. 47. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.
Finding #15	[redacted]
Finding #16	[redacted]

Finding	Recommendation
Finding #17	[redacted] 54. Define and implement a process to ensure the timely resolution of incidents. For example, establish routine status reviews for tracking incident response activities to completeness.
Finding #18	55. Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements: – performance of periodic reviews of risk designations at least annually – explicit position screening criteria for information security role appointments – description of how cybersecurity is integrated into human resources practices

Appendix A. Objective, Scope, and Methodology

A.1 Objective

The objective was to perform an independent evaluation of CPSC's implementation of FISMA for FY 2019. In support of this objective, Carson conducted a review in accordance with OMB MM 19-02, *Fiscal Year 2018 - 2019 Guidance on Federal Information Security and Privacy Management Requirements*, reporting guidelines.

A.2 Scope

The evaluation focused on reviewing CPSC's implementation of FISMA for FY 2019. The evaluation included an assessment of the effectiveness of CPSC's information security policies, procedures, and practices; and a review of information security policies, procedures, and practices of a representative subset of 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 CPSC's headquarters from May 2019 through September 2019. Any information received from 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 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 2019

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 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics
- FY 2019 Chief Information Officer Federal Information Security Modernization Act of 2014 Metrics

- FY 2019 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 800-30
- 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 800-44
- National Institute of Standards and Technology (NIST) SP 800-50
- 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 800-122
- National Institute of Standards and Technology (NIST) SP 800-128
- National Institute of Standards and Technology (NIST) SP 800-137
- National Institute of Standards and Technology (NIST) SP 800-161
- 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) *Supplemental Guidance on Ongoing Authorization*
- Office of Management and Budget Circular No. A-11
- 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, 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
- Office of Management and Budget, Memorandum 19-02
- Presidential Policy Directive - 41
- 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 Response

Finding 1: Inadequate Information Systems Inventory

Management concurs with this finding.

Finding 2: PIV Not Adequately Enforced

Management concurs with this finding.

Finding 3: Inadequate Information System Component Inventory

Management concurs with this finding.

Finding 4: Inadequate Implementation of Privileged User Controls

Management concurs with this finding.

Finding 5: Incomplete FICAM Roadmap

Management concurs with this finding.

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.

Management intends to continue working with DHS on CDM implementation with phase 2 having particular relevance to improvements to access management functions.

Finding 6: Ineffective Role-Based Training Requirements

Management concurs with this finding.

Finding 7: Inadequate ISCM Program

Management concurs with this finding.

Finding 8: No Existing Enterprise Architecture

Management concurs with this finding.

Finding 9: Ineffective Configuration Management

Management concurs with this finding.

Finding 10: Lack of Formally Documented Contingency Plans

Management concurs with this finding.

Finding 11: Inadequate Media Sanitization Procedures

Management concurs with this finding.

Finding 12: Inadequate Contract Language

Management concurs with this finding.

Finding 13: Organizational Level Risk is Not Adequately Managed

Management concurs with this finding.

Finding 14: Inadequate Plan of Actions and Milestones (POA&Ms) Documentation and Implementation

Management concurs with this finding.

Finding 15: Inadequate monitoring of inbound/outbound Traffic

Management concurs with this finding.

Finding 16: Inadequate Remote Access Log Review

Management concurs with this finding.

Finding 17: Inadequate Incident Response Capabilities

Management concurs with this finding.

Finding 18: Lack of Personnel Risk Designation and Screening Procedures

Management concurs with this finding.

Appendix C. Acronyms

AR	Accountability, Audit, and Risk Management
BCP	Business Continuity Plan
BIA	Business Impact Assessment
BOD	Binding Operational Directive
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
CIS	Center for Internet Security
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
DI	Data Quality and Integrity
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name Server
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	General Support System
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
IP	Individual Participation and Redress
ISCM	Information System Continuous Monitoring
ISCP	Information System Security Plan
IT	Information Technology
M	Memorandum
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
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connections
URL	Uniform Resource Locator

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:
301-504-7906
1-866-230-6229

On-line complaint form:
Click here for complaint form.
Click here for CPSC OIG Website.

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