



# Office of Inspector General

U.S. Consumer Product Safety Commission

## Evaluation of CPSC's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA 2014)

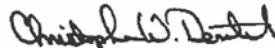
October 31, 2017



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

October 31, 2017

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

FROM: Christopher W. Dentel, Inspector General 

SUBJECT: Federal Information Security Modernization Act (FISMA) Evaluation

The Federal Information Security Modernization Act (FISMA) requires that the U.S. Consumer Product Safety Commission's (CPSC) Office of Inspector General (OIG) conduct an independent evaluation of the CPSC's information security program and practices.

To assess agency compliance with FISMA for FY 2017, the CPSC Office of Inspector General (OIG) 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 inspection be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Inspection and Evaluation (QSIE).

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 (DHS) and the Office of Management and Budget (OMB).

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

The OIG noted 13 findings in this year's FISMA review. These findings and the areas identified as requiring improvement are detailed in the attached report.

Should you have any questions, please contact me.

# Table of Contents

Executive Summary .....	iii
1. Objective.....	1
2. Background .....	1
3. Criteria.....	1
4. Evaluation Results .....	1
5. Findings .....	2
5.1 Finding 1: Lack of formally documented Contingency Plans.....	2
5.2 Finding 2: Insufficient documentation around configuration management.	4
5.3 Finding 3: Lack of enforcement of Personal Identity Verification (PIV) across the organization .....	5
5.4 Finding 4: No existing enterprise architecture documented for managing risk.....	7
5.5 Finding 5: Inadequate implementation of an asset inventory and supporting policies and procedures.....	8
5.6 Finding 6: Privileged user accounts are not provisioned and managed adequately .....	10
5.7 Finding 7: Risk from an organizational level is not adequately managed.	11
5.8 Finding 8: Contract language does not adequately identify requirements to mitigate risks.....	13
5.9 Finding 9: Lack of a defined strategy and milestones to align with Federated Identity, Credential, and Access Management (FICAM) and the implementation of DHS's CDM Program.....	14
5.10 Finding 10: Role-based training requirements are not adequately defined across the organization .....	15
5.11 Finding 11: No documentation to support the implementation of information security Program Management (PM) controls. ....	17
5.12 Finding 12: Plan of Actions and Milestones (POAMS) are not adequately documented and implemented. ....	18
5.13 Finding 13: Lack of defined and communicated security control implementations and ISCM activities.....	19
6. Recommendations .....	20
Appendix A. Objective, Scope, and Methodology .....	24
A.1 Objective .....	24
A.2 Scope .....	24
A.3 Methodology.....	24
Appendix B. Management Views on Conclusions and Findings .....	28
Appendix C. Acronyms.....	33

# List of Tables

Table 6-1: Index of recommendations ..... 20

# Executive Summary


The Federal Information Security Modernization Act of 2014 (FISMA 2014) 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 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. The Office of Management and Budget (OMB) requires OIGs to report their responses to OMB's annual FISMA 2014 reporting questions for OIGs via an automated collection tool.

The U.S. Consumer Product Safety Commission (CPSC) OIG retained Richard S. Carson & Associates, Inc. (Carson Inc.) to perform an independent evaluation of the CPSC's implementation of FISMA 2014 for Fiscal Year (FY) 2017. 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 the OMB.

## What We Found

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

- The CPSC allocated resources to define and document a formal organizational risk management plan.  
█ 
- Management has established a target date of March 2018 for the implementation of DHS' Continuous Diagnostics and Mitigation (CDM) to support the automation of managing software licenses.
- The CPSC is making progress with the development of a formal Enterprise Architecture, and the agency's focus is currently on boot strap data management and requirements as outlined via the Federal Enterprise Architecture (FEA).
- Management has made progress around risk management by establishing an Executive Risk function, led by the CPSC Chief Financial Officer (CFO) and

attended by the Chief Information Officer (CIO), the Chief Information Security Officer, and various mission executives to discuss topics around information security. Further efforts are in progress to document the adopted processes.

- The security and awareness training and role-based training efforts are continually being assessed to ensure compliance with existing policy and procedures.
- The CPSC continuously updates the Information Security Continuous Monitoring (ISCM) program in an effort to meet compliance with OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*.

We noted thirteen (13) 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 46 recommendations.

## 1. OBJECTIVE

---

The objective was to perform an independent evaluation of the CPSC's implementation of the FISMA 2014 for FY 2017.

## 2. BACKGROUND

---

On December 18, 2014, the President signed the FISMA 2014, which reformed the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 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 2014 requires the annual evaluation to be performed by the agency's OIG or by an independent external auditor. OMB Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 16, 2017, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The CPSC OIG retained Carson Inc. to perform an independent evaluation of the CPSC's implementation of FISMA 2014 for FY 2017. This report presents the results of that independent evaluation. Carson Inc. will also submit responses to OMB's annual FISMA reporting questions for OIGs to the CPSC OIG and the CPSC OIG will submit this information via OMB's automated collection tool in accordance with OMB guidance.

## 3. CRITERIA

---

Carson Inc. utilized the criteria established by the Federal Government to evaluate the CPSC's FY 2017 IT security program in accordance with FISMA 2014. 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 information technology 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 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 SOPs for the major systems have not been developed and distributed.

#### Criteria

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 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.



NIST Cybersecurity Framework (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 (5) 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 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 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:

1. 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).
2. 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.
3. Test the set of documented contingency plans.

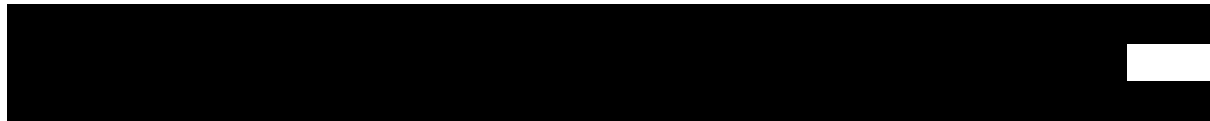
4. Integrate documented contingency plans with the other relevant agency planning areas.

## 5.2 FINDING 2: INSUFFICIENT DOCUMENTATION AROUND CONFIGURATION MANAGEMENT

### Condition

The CPSC relies on the General Support System Local Area Network (GSS LAN) Configuration Management (CM) policy and has documented a configuration management procedure. 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, 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.

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.



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

### Criteria

NIST SP 800-53, Revision 4, requires the organization to develop, document, and disseminate CM policies 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.

The CSF was established in part to foster risk and cybersecurity management communications. The CSF is mapped to NIST 800-53 and the SANS Top 20 set of controls. Center for Internet Security (CIS) 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 processes in an effort to prevent attackers from exploiting vulnerable services and settings.

The FY 2017 IG FISMA 2014 Reporting Metrics, v1.0 requires identification of TIC critical capabilities, as outlined via the TIC Reference Architecture Document, Appendix B.

### Cause

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

### Effect

Without a developed, documented, communicated, and implemented CM processes, the CPSC risks not maintaining the confidentiality, integrity and availability of assets supporting its mission.

### Recommendation

We recommend management:

5. Develop and enforce a CM plan to ensure it includes all requisite information.  
■ [REDACTED]
7. Identify and document the characteristics of items that are to be placed under CM control.
8. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of configuration changes.  
■ [REDACTED]
10. Further define the resource designations for a Configuration Control Board.
11. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service.
12. Fully implement the CM policies and procedures.

## 5.3 FINDING 3: LACK OF ENFORCEMENT OF PERSONAL IDENTITY VERIFICATION (PIV) ACROSS THE ORGANIZATION

### Condition

The CPSC has implemented a Virtual Desktop Infrastructure to enforce PIV card access systematically for many agency users. As established by process, network account passwords are not distributed to users. Exception protocols have been

established to assist users that may have lost a PIV card or experienced other technical issues.

[REDACTED]

### Criteria

Homeland Security Presidential Directive – 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* compels the agency-wide use of PIV credentials for logical and physical access.

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

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

### Cause

[REDACTED]

### Effect

[REDACTED]

### Recommendation

We recommend management:

[REDACTED]

## 5.4 FINDING 4: NO EXISTING ENTERPRISE ARCHITECTURE DOCUMENTED FOR MANAGING RISK

### Condition

Although the CPSC has documented a Risk Management Strategy, the CPSC has not defined an enterprise architecture or integrated this 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 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 (or 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.

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 approach for implementing the Enterprise Architecture by focusing on data gathering, which has delayed the implementation of NIST controls and the Federal Enterprise Architecture.

## Effect

The lack of an enterprise architecture to support managing risk at the organizational level increases risk and exposure for implementing current and future architecture states. Additionally, the lack of a Risk Executive Function may foster inconsistent management of risk across the organization, ultimately impacting the CPSC's mission success.

## Recommendation

We recommend management:

15. Develop an Enterprise Architecture to be integrated into the Risk Management Process.

## 5.5 FINDING 5: INADEQUATE IMPLEMENTATION OF AN ASSET INVENTORY AND SUPPORTING POLICIES AND PROCEDURES

### Condition

The CPSC has implemented various tools to support the establishment of a hardware and software inventory. These solutions include a property management system for tracking physical assets; a network inventory & integrated asset management solution to automatically scan the CPSC network for hardware and software; and a port scanner for detecting hardware. However, the following areas have not been addressed by the CPSC:

- Documented policies and procedures to support the requirements and process for developing and managing the inventories of major systems.
- A process documented to define how it monitors software license compliance. Currently, software license maintenance/compliance is manual and performed on an ad hoc basis.
- Process for defining a major system based on criteria outlined in OMB Circular A-130 (e.g., mission, cost, significant role, etc.) has not been documented.
- Defined a list of authorized hardware or software.
- Validation of the completeness/accuracy of the network inventory & integrated asset management solution output.

- Standard data elements (taxonomy) have not been defined and documented to support the existing inventory being maintained.

## Criteria

FISMA 2014 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 resources management.

NIST SP 800-53 also requires organizations to develop and maintain an inventory of its information systems.

Additionally, NIST SP 800-53 requires the following:

- A CM program which facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.
- An 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.

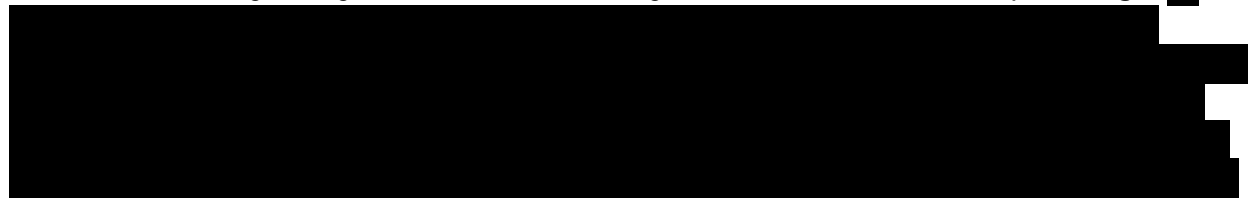
NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, outlines other requirements for the security-related information pertaining to a system component inventory.

## Cause

The CPSC has taken steps to improve asset management. While the CPSC has implemented technical solutions to support asset management, the implementation of the procedures for managing an inventory listing in accordance with NIST guidance will require additional resources and time.

## Effect

The lack of accurate and up-to-date hardware, software, and system inventories means the CPSC does not have a clear understanding of their system environment or the location of their assets. This could be problematic when recovering from facility, hardware, software, or system failures or security incidents which may result in recovery delays, increased recovery costs, and waste in IT planning. ■



## Recommendation

We recommend management:

16. Utilize the existing implementation of the Network Inventory and Integrated Asset Management solution to track and manage software licenses.  
[REDACTED]
18. 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).
19. Develop, document, and implement a process that identifies the CPSC's approach around determining and defining system boundaries.
20. Develop, document, and implement a process to classify agency systems as "major" or "minor" in accordance with OMB Circular A-130.  
[REDACTED]
23. Establish a policy and strategy to identify the CPSC's approach to manage software licenses around automated monitoring and expiry notifications.

### 5.6 FINDING 6: PRIVILEGED USER ACCOUNTS ARE NOT PROVISIONED AND MANAGED ADEQUATELY

#### Condition

The CPSC does not apply account management controls to support the Principle of Least Privilege and the 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 does not enforce the following:

- [REDACTED]
- Limiting the use of administrative accounts when performing non-administrative activities.  
[REDACTED]
- Automatic revocation of temporary and emergency accounts after a specified period of time.

The CPSC has not implemented the agency's Identification and Authentication (IA) policy designed to support the NIST SP 800-53 IA family of controls.



## Criteria

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

- [REDACTED]
- Removal of both temporary and emergency access automatically after a predefined period of time has elapsed.

## Cause

[REDACTED]

## Effect

[REDACTED]

## Recommendation

We recommend management:

- 26. [REDACTED]
- 27. Implement the identification and authentication policies and procedures.
- 27. Automatically revoke temporary and emergency access after a specified period of time.

## 5.7 FINDING 7: 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 ERM Playbook) or prioritized missions/business functions at the organizational level (level 1).

### Criteria

NIST SP 800-53 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 organization-level risk assessments to date.

### Effect

The lack of ranking and quantification of agency risks means the CPSC cannot efficiently and effectively direct resources to the most prevalent agency challenges.

## Recommendation

We recommend management:

28. Develop and implement an ERM program based on guidance from the ERM Playbook (A-123, Section II requirement).
29. 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.
30. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.

### 5.8 FINDING 8: CONTRACT LANGUAGE DOES NOT ADEQUATELY IDENTIFY REQUIREMENTS TO MITIGATE RISKS

#### Condition

The CPSC has developed an SOP that outlines the requirement for agency Contracting Officer Representatives (CORs) and the agency's Office of Information and Technology Services (EXIT) to coordinate with the procurement office 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 procedure, 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, 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 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, SA-4 requirements

## Criteria

NIST SP 800-53 requires the inclusion of acceptance criteria for information systems, information system components, and information system services, which are defined in the same manner as such criteria for any organizational acquisition or procurement, and are required to include references to the FAR.

## Cause

Management has not required the collaboration between the EXIT and the Division of Procurement Services to ensure the inclusion of required FAR clauses and NIST requirements and to update contract clauses as conditions change.

## Effect

This leaves the CPSC at an increased risk of security weaknesses arising from the service provider not being contractually obligated to meet IT security requirements.

## Recommendation

We recommend management:

31. 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.

## **5.9 FINDING 9: LACK OF DEFINED STRATEGY AND MILESTONES TO ALIGN WITH FEDERATED IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) AND IMPLEMENTATION OF DHS'S 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:

32. Define and document a strategy (that includes specific milestones) to implement FICAM.
33. Integrate the FICAM Strategy and activities into the Enterprise Architecture and ISCM.

## **5.10 FINDING 10: ROLE-BASED TRAINING REQUIREMENTS ARE NOT ADEQUATELY DEFINED ACROSS THE ORGANIZATION**

### **Condition**

The current CPSC's Awareness and Training Policy outlines requirements for CPSC staff, and this policy has been effectively implemented. The Talent Management System 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 the U.S. Code of Federal Regulations (5 CFR 930.301), role-based training must be provided to all personnel that affect security, which includes members of the Risk Executive Function, in addition to the all other applicable roles at the CPSC outlined in this CFR.

Additionally, the CPSC could not support that it has established and performed an adequate assessment of the knowledge, skills, and abilities of its workforce with significant security responsibilities. Also, the agency-specific policies, procedures, and responsibilities were not defined within the security awareness or role-based trainings provided by management. 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 requires the development, documentation, and implementation of security awareness and training policies and procedures that includes the following: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in support of the Awareness Training family of NIST 800-53 controls. NIST SP 800-53 also requires the dissemination of this policy to the appropriate stakeholders to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

As codified in 5 CFR 930.301 all roles that must affect security must be provided role-based security training. These roles include: executives, program and functional managers, CIOs, 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 are provided role-based training in accordance with the U.S. Code of Federal Regulations.

## Effect

Management has not adequately identified the personnel required to complete specialized or role-based training and this increases 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:

34. Perform an assessment of the knowledge, skills, and abilities of all CPSC personnel with significant security responsibilities.
35. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security (e.g., Executive Risk Council and the roles outlined in 5 CFR 930.301) are required to participate in role-based and/or specialized training.
36. Develop/tailor security training content for all CPSC personnel with significant security responsibilities.

37. Develop/tailor security awareness training and role-based security training content that reflects the agency's organization, requirements, types of systems, culture, mission, and risk environment.
38. Provide role-based security training to all CPSC users who affect security.

### **5.11 FINDING 11: NO DOCUMENTATION TO SUPPORT THE IMPLEMENTATION OF INFORMATION SECURITY PROGRAM MANAGEMENT (PM) CONTROLS.**

#### **Condition**

The CPSC has not documented the PM controls as required by NIST.

The existing System Security Plans (SSPs) for the five major systems defined by the CPSC have been updated to reflect the control baselines for a moderate categorization. However, no control implementation statements (e.g., common controls) were documented for the information security PM family of controls.

The CPSC does not maintain an organization-wide information security program plan which supplements the individual security plans developed for each of the major system SSPs.

#### **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 PM controls are described in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix G. These controls should be implemented at the organizational level.

#### **Cause**

Management's interpretation of the NIST guidelines for a moderate system was not fully aligned with the FISMA requirements. Therefore, the reference to NIST SP 800-53, Appendix G, requiring implementation, was not considered during the most recent review and update to the major system SSPs or the review of security controls.

#### **Effect**

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

## Recommendation

We recommend management:

39. Develop and distribute an organization-wide information security program plan.
40. Implement and assess the effectiveness of the PM controls, as documented in the information security program plan.

### 5.12 FINDING 12: PLAN OF ACTIONS AND MILESTONES (POAMS) 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 POAMs. Also, 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 metrics obtained via CSAM for the recorded POAMs 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, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires the development of a POAMs for the information system to document the organization's planned remedial 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 M 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, and changes to milestones.

#### Cause

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



## Effect

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

## Recommendation

We recommend management:

41. Establish and implement policies and procedures that require the documentation of POAMs with the OMB required level of granularity.
42. Establish appropriate dates to remediate issues reported and documented as part of the POAM process.
43. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.

### **5.13 FINDING 13: LACK OF DEFINED AND COMMUNICATED SECURITY CONTROL IMPLEMENTATIONS AND ASSOCIATED ISCM ACTIVITIES.**

#### Condition

CPSC has defined processes for performing assessments, authorizations, and monitoring for ISCM and has adopted a three (3) cycle assessment of controls. However, as alluded to above, the CPSC has not documented the establishment or assessed the implementation of all relevant security controls associated with all agency-defined major systems.

#### Criteria

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, 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 800-137 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 required to perform assess all required security controls.

**Effect**

This increases the risk of not identifying gaps associated with the known or identified security controls implementation.

**Recommendation**

We recommend management:

- 44. Perform a gap analysis to identify all NIST SP 800-53, rev 4 security controls that were not documented and assessed.
- 45. Document the implementation of all relevant security controls identified in the gap analysis.
- 46. Assess the implementation of all relevant security controls that were identified in the gap analysis.

**6. RECOMMENDATIONS**

---

*Table 6-1: Index of Recommendations*

Finding	Recommendation
Finding #1	<ul style="list-style-type: none"> <li>1. 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).</li> <li>2. 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.</li> <li>3. Test the set of documented contingency plans.</li> <li>4. Integrate documented contingency plans with the other relevant agency planning areas.</li> </ul>
Finding #2	<ul style="list-style-type: none"> <li>5. Develop and enforce a CM plan to ensure it includes all requisite information.  <div style="background-color: black; width: 100%; height: 1.2em; margin-top: 5px;"></div> </li> <li>7. Identify and document the characteristics of items that are to be placed under CM control.</li> <li>8. Establish measures to evaluate, coordinate, and approve/disapprove the implementation of configuration changes.  <div style="background-color: black; width: 100%; height: 1.2em; margin-top: 5px;"></div> </li> </ul>

Finding	Recommendation
	<p>10. [REDACTED]</p> <p>Further define the resource designations for a Configuration Control Board.</p> <p>11. Define and document all the critical capabilities that the CPSC manages internally as part of the TIC program Managed Trusted Internet Protocol Service.</p> <p>12. Fully implement the CM policies and procedures.</p>
Finding #3	[REDACTED]
Finding #4	15. Develop an Enterprise Architecture to be integrated into the Risk Management Process.
Finding #5	<p>16. Utilize the existing implementation of the Network Inventory and Integrated Asset Management solution to track and manage software licenses.</p> <p>[REDACTED]</p> <p>18. 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).</p> <p>19. Develop, document, and implement a process that identifies the CPSC's approach around determining and defining system boundaries.</p> <p>20. Develop, document, and implement a process to classify agency systems as "major" or "minor" in accordance with OMB Circular A-130.</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>23. Establish a policy and strategy to identify the CPSC's approach to manage software licenses around automated monitoring and expiry notifications.</p>
Finding #6	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>26. Implement the identification and authentication policies and procedures.</p> <p>27. Automatically revoke temporary and emergency access after a specified period of time.</p>

Finding	Recommendation
Finding #7	<p>28. Develop and implement an ERM program based on guidance from the ERM Playbook (A-123, Section II requirement).</p> <p>29. 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.</p> <p>30. Integrate the established strategy for identifying organizational risk tolerance into the ISCM plan.</p>
Finding #8	<p>31. 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.</p>
Finding #9	<p>32. Define and document a strategy (that includes specific milestones) to implement FICAM.</p> <p>33. Integrate the FICAM Strategy and activities into the Enterprise Architecture and ISCM.</p>
Finding #10	<p>34. Perform an assessment of the knowledge, skills, and abilities of all CPSC personnel with significant security responsibilities.</p> <p>35. Modify the Security and Awareness Training policy to ensure CPSC personnel that affect security (e.g., Executive Risk Council and the roles outlined in 5 CFR 930.301) are required to participate in role-based and/or specialized training.</p> <p>36. Develop/tailor security training content for all CPSC personnel with significant security responsibilities.</p> <p>37. Develop/tailor security awareness training and role-based security training content that reflects the agency's organization, requirements, types of systems, culture, mission, and risk environment.</p> <p>38. Provide role-based security training to all CPSC users who affect security.</p>
Finding #11	<p>39. Develop and distribute an organization-wide information security program plan.</p> <p>40. Implement and assess the effectiveness of the PM controls, as documented in the information security program plan.</p>
Finding #12	<p>41. Establish and implement policies and procedures that require the documentation of POAMs with the OMB required level of granularity.</p> <p>42. Establish appropriate dates to remediate issues reported and documented as part of the POAM process.</p> <p>43. Establish criteria to ensure analytics are performed on monthly reporting data and subsequently reported to management.</p>
Finding #13	<p>44. Perform a gap analysis to identify all NIST SP 800-53, rev 4 security controls that were not documented and assessed.</p>

Finding	Recommendation
	45. Document the implementation of all relevant security controls identified in the gap analysis. 46. Assess the implementation of all relevant security controls that were identified in the gap analysis.

## Appendix A. Objective, Scope, and Methodology

---

### A.1 Objective

The overall objective was established to assist the OIG in meeting its statutory obligation for independent, objective assessment of the CPSC's computer security programs in terms of program efficiency and effectiveness, policies and practices, and compliance with federal guidelines. In support of this objective, Carson Inc. conducted a high-level, qualitative review in accordance with OMB Memorandum M-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 2014 for FY 2017. 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 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 June 2017 through September 2017. 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 Inc. used a qualitative analysis for assessing the effectiveness of the Commission's efforts to secure its information systems. The evaluation included an assessment of the NIST Cybersecurity Framework Function Levels, as specified in

the *FY 2017 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, v1.0*:

- Identify (Risk Management)
- Protect (Configuration Management)
- Protect (Identity and Access Management)
- 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
- 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
- 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
- Federal Enterprise Architecture Framework, v2
- 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
- Federal Risk and Authorization Management Program - Standard Contract Clauses
- FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, v1.0
- Homeland Security Presidential Directive 12
- National Archives and Records Administration, *Guidance on Information Systems Security Records*
- National Cybersecurity Workforce Framework v1.0
- National Insider Threat Policy
- National Institute of Standards and Technology Cybersecurity Framework
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800- 50, *Building an Information Technology Security Awareness and Training Program*

- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-181 (Draft), *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-30, *Guide for Conducting Risk Assessments*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-34, *Contingency Planning Guide for Federal Information Systems*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-40, Rev. 3, *Guide to Enterprise Patch Management Technologies*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Rev 4., *Security and Privacy Controls for Federal Information Systems and Organizations*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-61 Rev. 2, *Computer Security Incident Handling Guide*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-63, *Digital Identity Guidelines*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- National Institute of Standards and Technology (NIST) Special Publications (SP) 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- National Institute of Standards and Technology (NIST) Supplemental Guidance on Ongoing Authorization
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
- Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*



- OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB M-08-05, *Implementation of Trusted Internet Connections*
- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB M-16-04, *Cybersecurity Strategy and Implementation Plan*
- OMB M-17-09, *Management of Federal High Value Assets*
- President's Management Council
- SANS Institute Critical Security Controls
- US-Computer Emergency Readiness Team - Federal Incident Notification & Response Guidelines

## **Appendix B. Management Views on Conclusions and Findings**

---

### **Finding 1: Lack of Formally Documented Contingency Plans**

*Management concurs with this finding.*

*Management completed development of individual contingency plans (ISCPs) for all major systems in FY 2017. Management plans to sign and distribute contingency 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 2018 using input from the individual BIAs.*

*Management has completed testing of individual contingency plans.*

*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.*

[REDACTED]

### **Finding 2: Insufficient Documentation around Configuration Management**

*Management concurs with this finding.*

*In FY 2017, Management completed development of individual Configuration Management plans and baseline configurations for all major systems. Management plans to sign and distribute Configuration Management plans in FY 2018.*

[REDACTED]

### **Finding 3: Lack of Enforcement of Personal Identity Verification (PIV) across the Organization**

*Management concurs with this finding.*

*Management implemented mandatory two-factor PIV authentication for all standard, non-privileged network access in FY 2017.*

[REDACTED]

[REDACTED]

**Finding 4: 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, 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 5: Inadequate Implementation of an Asset Inventory and Supporting Policies and Procedures**

*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 will explore ways to increase integration with our automated asset identification tool.*

*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.*

*Management performs an asset inventory annually to verify location and ownership of agency hardware.*

[REDACTED]

**Finding 6: Privileged User Accounts are Not Provisioned and Managed Adequately**

*Management concurs with this finding.*

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

*Current practices are substantially effective with respect to segregation of duties. Because of the limited number of agency technical support staff, system privileges and duties may extend beyond optimal support boundaries.*

[REDACTED]

**Finding 7: 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.*

*Management will work to improve the alignment of information technology risks with the enterprise risk management activities. Consistent with the cybersecurity risk framework.*

**Finding 8: Contract Language Does Not Adequately Identify Requirements to Mitigate Risks**

*Management concurs with this finding.*

*Management has in place internal operating procedures for procurement covering the specified FAR references identified in the description of this finding.*

*The finding references the lack of a policy or procedure to ensure that existing contracts have the required clauses however no known existing deficiencies relating to the FAR specific clauses were identified.*

*The finding references a lack of processes to affirm security controls provided by third parties. 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.*

*Management will review NIST 800-53, SA-4 and cloud related terms and conditions to determine the extent to which existing procedures may need modification.*

**Finding 9: 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.*

**Finding 10: Role-Based Training Requirements 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, or firewall administration or with management oversight of these programs including the CISO and CIO are considered to have significant security responsibilities and receive the appropriate role-based training.*

**Finding 11: No documentation to support the implementation of information security program management (PM) controls**

*Management concurs with this finding.*

*Management intends to review and document the implementation status of NIST SP 800-53 Program Management (PM) controls.*

**Finding 12: Remediation of Plan of Actions and Milestones (POA&Ms) are not consistently remediated**

*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.*

*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 report meets agency requirements.*

*Management intends to increase attention and prioritize resource allocation to further improve the timeliness of POAM item resolution.*

**Finding 13: Lack of defined and communicated ISCM activities.**

*Management concurs with this finding.*

*Management maintains that it followed NIST guidance in the assessment of agency information systems.*

*Management intends to address the program management controls identified in finding 11 however management contends that all relevant security controls associated with all agency-defined major systems have been assessed as required.*

*Management has developed and maintains an ISCM Plan that defines the specific information system metrics that are collected, monitored, and analyzed. [See Appendix D in the CPSC Information System Continuous Monitoring Plan].*

## Appendix C. Acronyms

---

BCP	Business Continuity Plan
BIA	Business Impact Assessment
Carson Inc.	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
COR	Contract Officers Representative
CP	Contingency 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
ERM	Enterprise Risk Management
EXIT	Office of Information Technology
FAR	Federal Acquisition Regulation
FCD1	Federal Continuity Directive 1
FEA	Federal Architecture Framework
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
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
IG	Inspector General
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 the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PM	Program Management
POAMs	Plan of Actions and Milestones
SDLC	System Development Lifecycle
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connection



# 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

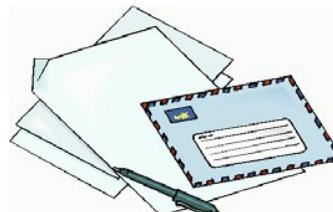


Click [here](#) for complaint form.

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





National Security Archive,  
Suite 701, Gelman Library, The George Washington University,  
2130 H Street, NW, Washington, D.C., 20037,  
Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)