U.S. CONSUMER PRODUCT SAFTEY COMMISSION

OFFICE OF INSPECTOR GENERAL

FY 2014 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW REPORT

Issued: 11/14/2014

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

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

Christopher W. Dentel
Inspector General

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

Date: November 14, 2014

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

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Federal Information Security Management Act (FISMA) Evaluation

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

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements. The CPSC's General Support System (GSS LAN) has completed the security accreditation process and retained an active security accreditation. In addition, the Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDS/RAM) application, and the CPSC public website, www.cpsc.gov, completed independent security assessments and retain active security accreditations.

Although much has been accomplished, a good deal of work remains. The OIG noted that management has not updated and approved all of the major applications' security documentation, even though management formally accepted the risk associated with operating these applications. Additionally, management has not fully implemented the National Institute of Technology and Standards (NIST) Special Publication (SP) 800-37, *Risk Management Framework*. Management has not accredited the information resources that reside outside of the GSS LAN security boundary. Management also has not performed an assessment to identify, categorize, accredit, and authorize the operation of all agency applications in accordance with OMB Memorandum M-10-15. It is particularly important that management assess the Division Epidemiology applications because of the applications' crucial importance to the agency mission and because of the potential of these applications to contain Personally Identifiable Information (PII). The OIG noted 53 findings, seven of which are considered high-risk, in this year's review. The IT challenges currently facing the agency are particularly relevant as the agency continues to deal with the implementation of the Consumer Product Safety Improvement Act (CPSIA) in general, and specifically with the CPSIA's impacts on the agency's IT operations.

Management continues to develop remediation strategies to address the known weaknesses, with a priority placed on what the Office of Information and Technology Services (EXIT) informally determines to be the highest risk issues. However, the full mitigation of these risks will require a significant amount of additional effort.

Should you have any questions, please contact me.

Christopher W. Dentel
Christopher W. Dentel
Inspector General

Table of Contents

FEDERAL INFORMATION MANAGEMENT ACT REPORT

EXECUTIVE SUMMARY

RESULTS OF THE EVALUTION

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

This year's FISMA evaluation found that management continues to make progress in implementing the FISMA requirements, although much work remains. The CPSC's General Support System (GSS LAN) has completed the security accreditation process and retained an active security accreditation. In addition, the Consumer Product Safety Risk Management System (CPSRMS), the International Trade Data System/Risk Automation Methodology System (ITDS/RAM) application, and the CPSC public website, www.cpsc.gov, completed independent security assessments and retain active security accreditations.

The agency's system monitoring and reporting capabilities have improved substantially since Fiscal Year (FY) 2010. The system reporting and monitoring, now possible, is far greater than it was in FY 2010 or even in 2013, and management has shown a strong commitment to continually improving these capabilities.

In 2014, management continued to improve the incident response process. The Cyber Security Incident Response Team, implemented by management in 2013, continues to improve its processes as it matures by refining Standard Operating Procedures (SOPs), improving the precision of existing metrics designed to assess the Incident Response Handling process, and implementing new solutions and improving existing solutions to facilitate the identification of security incidents. The agency's continually improving system reporting and monitoring capabilities, combined with the agency's maturing incident handling process, has positioned management to consistently take proactive steps to address known and potential vulnerabilities.

Although much has been accomplished, a good deal of work remains. The OIG noted that management has not updated and approved all of the major applications' security documentation, even though management formally accepted the risk associated with operating these applications in FY 2014. Additionally, management has not fully implemented the National Institute of Technology and Standards (NIST) Special Publication (SP) 800-37, *Risk Management Framework*. Management has not accredited the information resources that reside outside of the GSS LAN security boundary. Management also has not performed an assessment to identify, categorize, accredit, and authorize the operation of all agency applications in accordance with OMB Memorandum M-10-15. It is particularly important that management assess the Division Epidemiology applications because of the applications' crucial importance to the agency mission and because of the potential of these applications to contain Personally Identifiable Information

(PII). The OIG also noted 53 findings, seven of which are considered high-risk, in this year's review. The IT challenges currently facing the agency are particularly relevant as the agency continues to deal with the implementation of the Consumer Product Safety Improvement Act (CPSIA) in general, and specifically with the CPSIA's impacts on the agency's IT operations.

Management continues to develop remediation strategies to address the known weaknesses, with a priority placed on what the Office of Information and Technology Services (EXIT) informally determines to be the highest risk issues. The CPSC is in the process of remediating these issues. However, the full mitigation of these risks will require a significant amount of additional effort. For example, although management has developed policies, procedures and plans to improve the Continuous Monitoring process going forward, management did not update all the agency's major applications' security documentation in FY 2014, or periodically update each of the agency's Plan of Actions and Milestones (POAMs) in FY 2014. Additionally, management stopped generating the monthly reports that included threats, open POAMs, and major system changes in FY 2014. The Continuous Monitoring process will only continue to improve if: management optimizes its current tool set, continues to improve system reporting, addresses existing POAMs, and identifies new threats. This information, of course, must be shared with senior management.

In addition, management has not implemented Contingency Planning. Management has not developed a current Business Impact Analysis (BIA), and without a BIA, management cannot develop Business Contingency Plans, Disaster Recovery Plans, Information System Contingency Plans (ISCPs), or an agency Continuity of Operation Plan. Management has also not developed a workable Enterprise Architecture (EA), which is critical in mission planning, contingency planning, and risk management.

Management's Response

Management generally concurs with the findings outlined in the FISMA evaluation. The OIG agrees that the issues that management mentioned in its response are valid. However, the tasks outlined (developing a risk profile for security weaknesses and developing a cost-benefit analysis to determine the most effective approach to address the issues) are agency responsibilities and not within the scope of the OIG's evaluation. Also, management's interpretation of A-130 and NIST SP 800-53 does not consider the guidance promulgated by the Code of Federal Regulations, OMB and NIST. See Appendix A for management's official response.

INTRODUCTION

Background

On October 30, 2000, the President signed into law the FY 2001 National Defense Authorization Act, which included Title X, Subtitle G, the Government Information Security Reform Act (GISRA). On December 17, 2002, GISRA was superseded when the President signed into law the Electronic Government Act. Title III of this Act, the FISMA, along with the OMB policy referenced above, lays out a framework for annual IT security reviews, reporting, and remediation planning. FISMA seeks to ensure proper management and security for information resources supporting Federal operations and assets. The Act requires Inspectors General to perform an annual independent evaluation of their agency's information systems security programs and practices.

To establish a baseline to help it meet the requirements outlined above, the CPSC's OIG performed an independent review of the CPSC's automated information security control procedures and practices in FY 2014. The requirements of the review included:

- Evaluating and testing the internal controls defined in the 2014 FISMA metrics (provided by DHS);
- Testing the effectiveness of the information security controls defined in the 2014 FISMA metrics on all the CPSC's accredited, or previously accredited systems;
- Assessing whether the CPSC's information security policies, procedures, and practices comply with the Federal laws, regulations, and policies outlined in the 2014 FISMA metrics;
- Recommending improvements, where necessary, in security record keeping, internal security controls, and system security; and,
- Identifying the degree of risk associated with identified internal security controls weaknesses.

The review requirements also included tests of the entity-wide, system specific, and hybrid controls for the GSS LAN, www.cpsc.gov, CPSRMS, and ITDS/RAM systems, as defined in the 2014 FISMA metrics. The OIG used Federal standards and guidelines, including the guidance referred to in the 2014 FISMA metrics, to assess the design and effectiveness of the CPSC security controls. The objective of the review was to determine whether the CPSC's automated information system was adequately safeguarded.

In this report, the OIG identified security weaknesses in the CPSC's management, operational, and technical controls policies, procedures, and practices. The conditions of these controls could permit the modification or destruction of data, disclosure of sensitive information, or denial of services to users who require the information to support the mission of the CPSC.

To ensure proper coverage and mitigation of the risks identified by the DHS, the CPSC is required to perform its own testing procedures in order to assess the design and implementation of the DHS defined FISMA requirements. The CPSC OIG interviewed agency personnel, reviewed the 2014 GSS LAN, CPSRMS, ITDSRAM, and www.cpsc.gov security documentation (when available), reviewed system reports, and observed system configurations.

Objective

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

Scope

To accomplish our objective, our evaluation focused on the CPSC's information security program, the FY 2014 FISMA reporting metrics developed by DHS dated December 2, 2013, and the related requirements outlined by OMB, DHS, NIST, the Department of Commerce, the Federal Emergency Management Agency, and the Federal Chief Information Officer (CIO) Council. We conducted our evaluation from July 2014 to October 2014 at the CPSC's headquarters, located in Bethesda, Maryland. The OIG focused this evaluation within the boundaries of the GSS LAN, CPSRMS, ITDSRAM and www.cpsc.gov systems.

Methodology

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

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

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

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

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

This evaluation constitutes both a follow-up of the findings and recommendations resulting from earlier audits, and a review of the CPSC's implementation of the IT security criteria as currently defined by FISMA. However, this year's evaluation does not consider the status of the CPSC Data Privacy Program, as current DHS guidance, this year does not require this reporting by the OIG.

The statuses of each of these topics were reviewed and discussed with the CPSC's Chief Information Officer, Director of Information Technology and Technical Services (ITTS), Information Systems Security Officer (ISSO), and relevant members of their staffs. Documentation developed by both the CPSC officials and contractor personnel was reviewed. The documentation identified below was reviewed, as necessary, for the testing of the required FISMA areas:

- ✓ continuous monitoring solution configurations and reports
- ✓ configuration baselines and scan/exception reports
- ✓ user inventory reports
- ✓ incident response reports
- ✓ POAM reports
- ✓ user agreements
- ✓ property reports
- ✓ backup reports
- ✓ employee and contractor rosters
- ✓ Memorandum of Agreements (MOUs) and Interconnection Security Agreements (ISAs)
- ✓ CPSC OMB Exhibits 53/300
- ✓ planning documents
- ✓ vulnerability reports and system scanning results
- ✓ change control forms
- ✓ risk documents
- ✓ security training content/reports
- ✓ system configurations
- ✓ contingency plans
- ✓ system inventories
- ✓ agency templates
- ✓ contracts and Statement Of Works (SOWs)
- ✓ agency spending plans
- ✓ meeting minutes

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

RESULTS OF EVALUATION

Risk Management

FISMA requires security authorizations for all systems operated by the agency. FISMA also requires management to assess and monitor security controls on a continuous basis using a risk based approach based on, amongst other guidance, Federal Information Processing Standards (FIPS) 199, FIPS 200, FIPS 201, NIST SP 800-37, NIST SP 800-39, and NIST SP 800-53. Once management performs the initial authorization of a system, management should use the results of the on-going security assessments and monitoring tasks as a basis for each system's continuing Authorization To Operate (ATO).

Progress:
Management operated CPSRMS and ITDSRAM in 2014 with an expired ATO. As part of the reauthorization effort, management entered into a contract with a vendor to perform an independent assessment of these solutions. Management then reauthorized the CPSRMS and ITDSRAM applications to operate in FY 2014 based on this assessment. In addition, management certified the continued operation of the GSS LAN and cpsc.gov in 2014.

Issues To Be Addressed:

- Management has not developed policies and procedures to govern the agency's Risk Management process.
- Management has not established a comprehensive governance structure and organization-wide risk management strategy. For example:
  - Management has not established a Risk Executive (function), nor has management developed an organization-wide risk management strategy to ensure risks to the mission and organization are considered.
  - Management has not developed an EA and integrated the EA into the agency's risk management process.
  - Management has not developed and implemented an adequate process to define and accept risk when authorizing a system to operate.
    - Management has not defined the organizational risk tolerance or a process to determine if existing risks are within the organizational risk tolerance.
    - Management has not defined objective and measurable criteria used to justify the accreditation and reaccreditation, or conversely, decertification of in-scope systems.
    - Management assigns criticality to the security weaknesses on the POAM based on an undocumented, informal process.
  - Management has not documented the process by which it determines if existing risks are within the organizational risk tolerance.
- Management has not developed an inventory of major applications and provided the inventory to the Agency Head for certification, as required by FISMA, section 3505(c)(2).
- Management has not inventoried or categorized the CPSC's minor applications. Additionally, management has not selected, implemented, or assessed the security controls employed by the minor applications, or authorized the operation of the minor applications.

- Management has not updated all of the relevant security documentation (e.g., Categorization documents, System Security Plans (SSPs), Risk Assessments, etc.) for the GSS and each of the major applications in FY 14. Management does not, as a matter of practice, update security documents throughout the year to provide an up-to-date view of the information systems' security posture and provide a method of continuously monitoring those postures, as required by NIST SP 800-37.
- Management does not perform and document a Security Impact Analyses (SIA) for each system change, or update security documentation with the results of these assessments as required by NIST SP 800-37 and agency policies.
- Management did not develop periodic security status reports in FY 2014 that include the following:
  - the effectiveness of the existing security controls and changes to the GSS LAN, CPSRMS, ITDSRAM, and www.cpsc.gov systems;
  - current and emerging threats to assist in the mitigation of the risks posed by these threats; and
  - a summary of the agency software/hardware inventory.
- Management has not assessed or accredited the mission-critical resources that reside outside of the GSS LAN security boundary. These resources reside on an outside network, which does not use a Managed Trusted Internet Protocol Service connection.
- Management did not include all of the OMB and NIST-required information in the existing risk management documentation. For example, management has not defined the GSS LAN accreditation boundary in the GSS LAN security plan.

Risk Management Recommendations:

1. Management should develop and implement stand-alone risk management policies and procedures.

2. Management should develop and document a robust risk management process led by a Risk Executive (function). The Risk Executive function should report to a governing board that includes senior management. Management should also develop and implement a Risk Management Strategy using the NIST SP 800-37 guidance. The organization-wide Risk Management Strategy should include:
   a) Techniques and methodologies the organization plans to employ to assess information system related security risks and other types of risk of concern to the organization;
   b) Methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment;
   c) The types and extent of risk mitigation measures the organization plans to employ to address identified risks;
   d) The level of risk the organization plans to accept, i.e., risk tolerance;
   e) The methods and techniques the organization plans to use to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and,
   f) The degree and type of oversight the organization plans to use to ensure that management is effectively implementing the risk management strategy.

3. Management should document and certify a systems inventory that includes all CPSC systems and includes a description of each. The systems inventory description should include:
    a) The interfaces with all other systems/networks,
    b) The system criticality (based on a current BIA),
    c) The security categorization (based on FIPS 199),
    d) The hardware used by the system,
    e) The databases used by the system,
    f) The ATO status of each system, and
    g) The name of the system owner.

4. The agency head should review the system inventory annually and whenever a major change occurs. Ultimately, this inventory should tie to the solutions architecture in the EA.

5. Management should inventory and categorize each of the CPSC minor applications.

6. Management should select, implement, and assess the security controls employed by each of the CPSC minor applications. Management can include this information in the existing SSPs, where appropriate.

7. Management should formally authorize the operation of the minor applications once the minor applications' security controls are implemented.

8. Management should update and actively maintain all relevant security documentation, including SSPs, Security Assessment Reports (SARs), Risk Assessments, and POAMs, for the agency-defined major applications and General Support Systems.

9. Management should provide the updated security documentation to the Authorizing Official to reauthorize the GSS and major applications to operate.

10. Management should update the agency SSPs to include the accreditation boundaries.

11. Management should perform and document Security Impact Analyses (SIA) for system changes. The SIAs must include a sufficient level of detail to allow the CPSC security team to make a determination of the system change's impact on the agency's control environment.

12. Management should update all relevant security documentation (including baseline configuration documents, SSPs, SARs, Risk Assessments, and POAMs) each time a change with a security impact is made. Management should also update all relevant security documentation upon the completion of the annual security assessment. In general, the agency should maintain SSPs and other relevant risk documents as "living documents" to facilitate ongoing risk management decisions.

13. Management should enhance its periodic security status reporting to include a description of the results of the all ongoing monitoring activities performed by the agency. NIST requires

that at minimum, the security status reports should describe or summarize the results of the SIAs, key changes to SSPs, SARs, and POAMs. These reports should include:

a) A summary of the assessment of control effectiveness and changes to the GSS LAN CPSRMS, ITDSRAM, and cpsc.gov systems;
b) Any additions/changes to agency POAMs within the previous period;
c) A summary of the agency's hardware and software inventory;
d) Any new threats (e.g. from the Internet Storm Center, US-Cert notifications etc.); and
e) System changes with a security impact and the results of the associated SIAs.

14. Management should develop a comprehensive EA and integrate the EA into the risk management process. In addition, management should tie all system changes to the EA.

15. Management should appoint a "Change Manager" to provide governance to the change control process, as is recommended in NIST SP 800-100.

16. Management should provide training to resources responsible for implementing system and configuration changes. Management should train these resources on the CPSC change management procedures, and specify what information management requires when documenting a configuration change in a change management form.

17. Management should apply adequate security to the unaccredited resources located at the lab and accredit these resources in accordance with the relevant NIST and OMB guidance. Management may accomplish this by:
    a) Reintegrating these resources back into the GSS LAN and ensuring compliance with all agency policies; or
    b) Designing and implementing security controls using a separate security function and structure to ensure that the lab network on which the resources run is in accordance with all applicable NIST and OMB guidance.

Plan of Action and Milestones

OMB requires agencies to create and maintain POAMs for all known IT security weaknesses and report the status of the associated remedial actions to senior management on a quarterly basis. Despite these requirements, the CPSC is not documenting all of the OMB required data for each reported security weakness, or ensuring that all of the data entered is updated and reported to senior management in a timely manner. In addition, management has not integrated the funding of the agency POAMs into the Capital Planning process.

Progress:
Management hired a second Information Security Analyst in FY 2013 to assist with the administration of the IT security program, including the oversight of remedial actions and the maintenance of the CPSRMS and ITDS/RAM POAMs. However, the new Information Security Analyst left the agency in July 2013, and management has not refilled the position. Therefore, management decided to contract some of these services out in 2014. As part of the vendor’s

contract, the CPSRMS, ITDS/RAM, and www.cpsc.gov POAMs were updated for the agency's annual effort to reauthorize these systems to operate.

Issues To Be Addressed:

1. Management does not adhere to the estimated completion dates for each of the weaknesses identified in the agency POAMs.

2. The agency POAMs do not contain all of the OMB M-04-25 required information.

3. The program officials responsible for maintaining agency POAMs did not update the agency POAMs and provide the CIO with POAM updates on a quarterly basis throughout FY 2014.

POAM Recommendations:

1. Management should prioritize the remediation of security weaknesses and hold those charged with this remediation accountable for the timely completion of these tasks.

2. Management should perform an assessment of the level of effort required for the remediation of each security weakness, and the results of that assessment should be reflected in the milestone/milestone dates and "Estimated Completion Date" fields in the associated POAMs.

3. Management should ensure that all required POAM fields are completed for all security weaknesses.

4. Management should provide the updates to the CIO on all agency POAM activities on a quarterly basis.

Continuous Monitoring

In an effort to ensure agencies develop processes for real-time risk management and monitor their security posture on a continuous basis, OMB issued, amongst other guidance, OMB Memorandum M-14-03, and NIST issued, amongst other guidance, NIST Special Publications 800-37, 800-39, and 800-137.

Progress:

Management contracted with a vendor to develop a Continuous Monitoring Plan in FY 2014, perform an independent test of one-third of the GSS LAN, CPSRMS, ITDS/RAM, and www.cpsc.gov security controls, develop an Information Security Continuous Monitoring (ISCM) gap analysis, develop an ISCM Risk Assessment, and develop a ISCM strategy in 2014 to address the new requirements described in OMB M-14-03. Management also developed testing schedules and Security Assessment Plans for each of the aforementioned systems. Management presents monthly reports to program officials outlining current known vulnerabilities and the results of some of the agency's existing continuous monitoring activities. These reports include the results of periodic configuration compliance audits to identify United States Government Configuration Baseline/Federal Desktop Core Configuration variances, as well as the results of periodic patch and vulnerability assessments. This process will continue to improve as management implements new monitoring tools and optimizes its existing tool set. Management intends to have the program fully implemented by 2017 as part the phased approach described in OMB M-14-03.

Issues To Be Addressed:

- Management has not implemented the ISCM policy.
    - Management has not assessed Organizational Risk Tolerance to ensure that authorization decisions and updates to the ISCM are made within the Organizational Risk Tolerance.
    - Management has not updated all of the relevant security documentation for the GSS and each of the major applications in FY 14.
    - Management does not conduct SIA, which the ISCM policy requires. It should also be noted that NIST SP 800-37 requires agencies to perform SIAs as part of a comprehensive continuous monitoring approach.
- Management did not document an ISCM strategy by the February 28, 2014 deadline established in OMB M 14-03. The ISCM strategy that was documented after February 28, 2014 did not address the US-CERT Concepts of Operations (CONOPS) requirements.
- The scope of the ISCM Risk Assessment does not include the agency's major applications.

Continuous Monitoring Recommendations:

1. Management should implement the Risk Executive function and integrate that function into the Continuous Monitoring Process. Management should use this new function to assess organizational risk tolerance and integrate the organizational risk tolerance into the ISCM program.

2. Management should perform SIAs on all actual or proposed system changes. Management should document these results, along with the results from all other continuous monitoring activities in the monthly Security Status Reports. Management should also update the risk documentation accordingly.

3. Management should regularly update agency security plans and POAMs, and the security plans and POAMs should act as “living documents” in order to represent the most up-to-date security information related to the CPSC systems.

4. Management should update the ISCM strategy to include all of the CONOPS requirements.

5. Management should implement all aspects of the new ISCM strategy.

6. Management should perform a risk assessment on the CPSC ISCM strategy that includes the risks associated with the agency's major applications. This risk assessment should consider the indigenous risks associated with each system to ensure that management does not over/under allocate security efforts to any of its systems.

Contingency Planning

FISMA requires that management develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. However, management has not developed a Contingency Planning Program. Management is reviewing cloud technology solutions to remediate these issues and expects to begin performing these tasks in 2015.

Issues To Be Addressed:

- Management has developed a Contingency Planning Policy. However, management has not reviewed the policy in FY 2014 and the policy does not enumerate all of the test, training, and exercise (TT&E) program requirements defined in FCD1.
- Management has not implemented the CPSC Contingency Planning Policy:
    - Management has not developed a current and formal BIA;
    - Management has not established, documented, formalized or tested a Disaster Recovery Plan, Business Continuity Plan , or Continuity of Operations Plan;
    - Management has not established, documented, formalized or tested Information System Contingency Plans (ISCPs) for all agency systems;
    - Management has not reviewed and updated the all of the agency's existing ISCPs in FY 2014;
    - Management has not adequately tested the agency's existing ISCPs; and,
    - Management has not established an Alternative Processing Site.
- Management does not employ backup strategies to meet the Recovery Point Objectives (RPOs) documented in the ISCP. Specifically, the RPOs documented in the GSS LAN ISCP cannot be achieved with the management's current backup schedules.

Contingency Planning Recommendations:

1. Management should enhance its Contingency Planning Policy and procedures to address all NIST and OMB requirements. EXIT management should solicit input from each of the CPSC departments when developing these policies and procedures to ensure proper coverage.

2. The CPSC should develop a stand-alone test, training, and exercise policy to govern the agency's TT&E program; alternatively, the agency could enhance the existing Contingency Planning Policy to include TT&E requirements.

3. Management should train all of the relevant resources on the continuity planning responsibilities assigned to them in the policy.

4. Management should perform, document, and approve a formal Business Impact Analysis in accordance with NIST SP 800-34.

5. Management should establish, document, test, and approve a Disaster Recovery Plan, Business Continuity Plan, and Continuity of Operations Plan in accordance with NIST SP 800-34.

6. Management should establish, formalize, and test an ISCP for all critical agency systems in accordance with FEMA and NIST guidance.

7. Management should implement a solution to allow management to meet the documented RPOs for all critical systems.

8. Management should draft after-action reports to document the “lessons learned” that are identified as part of the Continuity Of Operations Plan, Disaster Recovery Plan, and Business Continuity Plan testing.

9. Management should establish an alternative processing site. This site should contain the equipment and supplies required to recommence operations in time to support the organization-defined time period for resumption.

Contractor Systems

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

Issues To Be Addressed:

- The Contractor Security Oversight policy was not reviewed or updated in FY 2014, and is missing the following information:
  - The process by which management controls cloud-based SaaS implementations.
  - A requirement for management to assess all third party systems' compliance with FISMA. FISMA compliance requires management to assess all related user controls, and for management to accredit these systems. Management should also develop procedures to guide this process.
  - The frequency that management must review/update agency MOUs/ISAs.
- Management has not fully implemented the Contractor Security Oversight Policy:
  - Management has not established processes and procedures to track various interagency service agreements and metrics that will be applied throughout the lifecycle of the many different and disparate IT security services within the organization;
  - Management does not notify third parties of intrusions, attacks, or internal misuse, so the third party can take steps to determine whether its system has been compromised;

    - Management does not analyze audit logs to detect and track unusual or suspicious activity across the interconnection that might indicate intrusions or internal misuse as is required by the Contractor Oversight Policy;
    - Management does not use automated tools to scan for anomalies, unusual patterns, and known attack signatures across the interconnection and to alert administrators if a threat is detected;
    - The ISSO or delegate does not periodically review audit logs to detect patterns of suspicious activity that scanning tools might not recognize;
    - EXIT does not coordinate contingency planning, training, testing, and exercises with any third party contractors to minimize the impact of disasters; and,
    - EXIT has not established joint procedures with third parties based on existing contingency plans.
- Management has not developed Security Plans for its third party solutions, assessed for compliance with third party solution user controls, or accredited its third party solutions.
- Management did not develop a Security Plan for an outside vendor, who connects with the agency network, or establish and approve an MOU or ISA with this vendor. Management also did not verify the vendor’s implementation of the security controls specified in the CPSC information security policies or accredit this solution.

Contractor System Recommendations:

1. Management should update the Contractor Oversight Policies and Procedures to include the following:
    a. The process by which cloud-based SaaS implementations are controlled.
    b. A requirement for management to assess all third party systems' compliance with FISMA. FISMA compliance requires management to assess all related user controls and for management to accredit these systems. Management should also develop procedures to guide this process.
    c. The frequency that management must review/update agency MOU/ISAs.

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

3. Management should notify third parties of intrusions, attacks, or internal misuse, so the third party can take steps to determine whether its system has been compromised.

4. Management should include a requirement in each ISA compelling the connecting third parties to provide the CPSC with the known security weaknesses that might have an impact on the agency's mission.

5. Management should analyze audit logs to detect and track unusual or suspicious activity across the interconnections that might indicate intrusions or internal misuse.

6. Management should implement automated tools to scan for anomalies, unusual patterns, and known attack signatures across the interconnection; and, management should configure these tools to alert administrators of detected threats.

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

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

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

10. Management should develop Security Plans for each of its third party solutions, have an independent assessment performed to ensure the design and effectiveness the user controls documented in the Security Plan, and accredit each of its third party solutions.

11. Management should either provide all outside vendors who connect to the agency network with CPSC laptops or accredit the vendor systems connecting to the CPSC network and establish an approved information system connection or processing agreement.

12. Management should update the Contractor Security Oversight policies/procedures to explicitly address what management must do to ensure that all documented user control considerations for each of the third party IT systems are considered.

Security Capital Planning

The CPSC Capital Planning process is based primarily on OMB Circular A-11, *Preparation, Submission, and Execution of the Budget,* and the OMB Capital Planning guide, which define the policies for planning, budgeting, acquiring, and managing Federal capital assets. The Information Technology Investment Management (ITIM) Directive, Capital Planning and Investment Control (CPIC) Guide, the System Development Life Cycle (SDLC) Guide, and the Project Management Office (PMO) Guide provide resources with internal policies and procedures for planning, budgeting, managing, and maintaining the agency’s portfolio of investments as critical assets for achieving agency strategic goals and missions. The agency has also developed an Investment Review Board (IRB) Charter, which describes the roles and responsibilities for the agency decision makers in the investment process and provides these resources with the authority to act.

Progress:
The OIG contracted Withum Smith+Brown (WS+B) to perform an Information Technology Investment Management (ITIM) assessment in FY 2013, which included an audit of the CPIC process. At that time, WS+B reported that the agency’s Investment Maturity Level was at stage one, the lowest of the five stages of the ITIM framework. Management agrees that this area remains a work in progress, and management is in the process of improving the process and developing and implementing new CPIC policies and procedures.

Issues to be addressed:

- The agency's capital planning policies and procedures are out-of-date, missing key elements, and have not been fully implemented.
  - Although the SDLC guide requires that each development project include the costs associated with all aspects of the security program, including POAM costs, the policies and procedures do not define how management plans and budgets for ongoing security costs, such as costs to perform the remediation activities outlined in the agency's POAMs. In addition, the policies and procedures do not compel management to cross-reference the POAM costs to the capital planning materials sent to OMB in the fall, as is required by OMB Memorandum M-11-33.
  - Management has not reviewed and updated the CPIC guide in FY 2014 and it does not represent the current process.
  - Management has not implemented the EA Guide referenced in the IT Investment Management Directive and the SDLC guide.
- Management has not, as required by OMB, provided funding for the remediation of existing security weaknesses before funding new initiatives.
- Management has implemented several new initiatives in FY 2014, although security weaknesses have remained outstanding for years.
- Although management budgets for identified needs, management does not sufficiently plan to ensure that information security resources are available for all expenditures.

Security Capital Planning Recommendations:

1. Management should update and implement existing agency Capital Planning and Investment Control policies and procedures, including the CPIC guide, SDLC guide and the EA guide. These guides should be consistent with OMB M-00-07.

2. Management should enhance and implement existing policies/procedures to ensure that the costs associated with remediating security weaknesses are properly cross-referenced to the capital planning materials sent to OMB.

3. Management should enhance and implement existing policies/procedures to require agency personnel to document the appropriate investment's Unique Investment Identifier in each POAM. This will facilitate traceability from the agency's POAMs to its capital planning documentation.

4. Management should enhance and implement existing policies/procedures to require all POAMs to reflect the estimated resource needs for correcting reported weaknesses and to specify whether funds will come from a reallocation of base resources or a request for new funding.

5. Management should develop and submit a Project Initiation Form for each outstanding security weakness identified on the agency POAMs, thus requiring the submission of said projects to the IRB for its consideration.

6. Management should document the Unique Investment Identifiers associated with each security weakness in the agency POAMs and record the cost to remediate the weakness in the

appropriate investment. This is to link the security costs for a system to the security performance of a system.

7. Management should fund and remediate all existing POAMs prior to investing in new development projects.

8. Management should ensure that information security resources are planned and available for all expenditures.

Configuration Management

Management monitors agency compliance with the United States Government Configuration Baseline (formally, the Federal Desktop Core Configuration) and the CPSC configuration management policies and procedures through its continuous monitoring program. Specifically, management includes configuration and patch management data for Windows 7 clients, CPSC servers, and selected hardware in the monthly Security Status Report. However, management has not properly documented or implemented baseline configurations for all agency software and hardware components.

Progress:
Although management has not implemented Defense Information System Agency (DISA) configuration settings to all agency systems, management has made significant progress in this endeavor. In addition, management has implemented a formal review over local administrator rights to workstations. Also, although management did not perform scans in November 2013 and April 2014, the CPSC has greatly improved its automated scanning capabilities, and reports these results to management on a monthly basis. These enhancements will, among other things, reduce the agency's attack surface, assist management in detecting/preventing attacks, reduce amount of unauthorized software on the network, improve software license compliance, and reduce the effort required to develop a comprehensive software inventory until management can implement an application whitelisting solution.

Issues to be addressed:

- The CPSC Configuration Management Policies are missing key elements, and management has not developed and implemented SOPs for the Configuration Management process. The Configuration Management policies or procedures do not include the following:
    - An organization-defined set of circumstances when baselines must be updated, and an explicit requirement for baselines to be updated as an integral part of information system component installations and upgrades.
    - A requirement for management to develop and document an inventory of information system components that includes organization-defined information deemed necessary to achieve effective information system component accountability; and a requirement that management reviews and updates the information system component inventory as frequently as determined necessary by the organization.

- o A requirement for management to take action when unauthorized components are detected by disabling network access by such components; isolating the components, and/or notifying appropriate agency personnel.
- o Also, management has not developed Configuration Management procedures, and the link that references the Configuration Management procedures is broken.
- o The frequency which management must review/update the Configuration Management Policies and Procedures.

- – Management does not maintain a comprehensive hardware and software inventory. In addition, management has not purged all unauthorized software installed on the CPSC network or developed a process to ensure software license compliance.
- – Management has not developed an inventory of software and hardware components requiring configuration baselines, and management has not baselined all agency software and hardware component configurations.
- – Management has not updated all of its existing configuration baseline documents in FY 2014.
- – The agency does not remediate or formally accept the risk associated with all non-compliances identified in the monthly DISA and patch management scans.
- – Management does not adequately test, validate, and document production changes:
  - a. Management does not consistently document the implementation date ("Date Change Made") in the change control forms.
  - b. Management does not adequately document the test steps performed to agency changes, including server patches.
  - c. Management does not adequately perform and document Security Impact Analyses on changes.
  - d. The ISSO does not consistently approve changes.
  - e. Management does not audit change control activities.
- – Management does not implement server, database, and widely used third party application patches in a timely manner. Additionally, management is using versions of databases that are not supported and the vendor is no longer patching.

Configuration Management Recommendations:

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

2. The agency should implement a solution to develop, approve, and maintain a current and comprehensive software/hardware inventory. Management should then assign ownership to all agency software/hardware.

3. Management should develop, approve, and maintain a target software/hardware inventory. This, along with recommendation 2, above, should be done with the assistance of the business owners. Business owners should identify Mission Essential Functions and systems and provide this information to EXIT. Thereafter, EXIT should identify and inventory the software and hardware associated with these functions.

4. Management should document the process for developing the software/hardware inventory in a procedure document.

5. Management should purge the network of all unauthorized software.

6. Management should implement a whitelisting or VDI solution to prevent systematically unauthorized software from running on the network.

7. Management should patch all software identified in the software inventory.

8. Management should implement the DHS Continuing Diagnostics and Mitigation Program once it becomes available.

9. Management should develop and enforce a process to govern software license compliance:
    a. Management should document and maintain a comprehensive software inventory.
    b. Management should document the number of instances of each type of software installed on the network.
    c. Management should document and inventory all software licenses owned by the agency.
    d. Management should reconcile the software instances installed on the network to the software licenses owned by the CPSC and remediate any discrepancies.
    e. Management should perform periodic audits to ensure compliance.

10. The CPSC should develop an inventory of software and hardware components requiring baselining, and the process for developing this inventory should be documented in a procedure document.

11. The CPSC should establish, document, and implement mandatory configuration settings (CM-2 and CM-6) for information technology products employed within the information system. The CM-6 configuration settings should use defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

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

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

14. Thereafter, management should monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

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

16. Management should document the implementation date for each production change.

17. Management should perform and document testing on each production change. This should include use cases, use case results, integration testing results, etc.

18. Management should provide training to personnel responsible for implementing system and configuration changes. Management should train these personnel on the CPSC change management procedures, and what information management requires when documenting a configuration change in a change management form (e.g. test cases, test methodologies, test results, etc.).

19. Management should perform and document SIA for each system change. The SIA should include a sufficient level of detail to allow the CPSC security team to make a determination of a system change’s impact to the agency’s control environment.

20. The ISSO or delegate should approve all system changes.

21. Management should audit production changes periodically to validate that the agency has adequately tested, documented, and approved the production changes.

22. Management should develop a comprehensive EA and management should tie all system changes to the EA.

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

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

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

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

27. Management should upgrade all unsupported versions of databases to supported versions of databases.

28. Management should require all external network traffic to be routed back through the Managed Trusted Internet Protocol Service connection.

29. Management should remediate all non-compliances with the baseline configurations and missing patches identified as part of monthly scans.

30. Management should implement and document controls to mitigate the risk posed by the accepted variances to the configuration baselines and missing patches identified in the monthly scans.

Incident Response and Reporting

Management has established incident detection, handling, and analysis policies and procedures. Management has also implemented an Incident Reporting database, to track incident reports documenting known security incidents. In addition, management has assigned resources to a Computer Security Incident Response Team (CSIRT) in accordance with the Incident Response policy. The CSIRT analyzes, validates, and documents all known security incidents. Additionally, management notifies US-CERT of security incidents. Management also uses a Security Information and Event Management solution to manage security logs and identify security incidents.

Progress:
Management has made substantial progress in implementing Incident Response and Reporting in FY 2014. Management has fully implemented the Incident Response policies and procedures, and responds to and resolves incidents in a timely manner. In addition, management developed a tool to streamline incident reports to US-CERT to ensure timely compliance with US-CERT CONOPS.

Issues to be addressed:
None

Security Training

EXIT administers the CPSC Security Awareness Training Programs using the Talent Management System (TMS). Specifically, EXIT verifies that all CPSC employees and contractors receive the required annual IT security awareness training. EXIT also provides specialized security training for EXIT employees who have significant information system security responsibilities.

Progress:
Management obtained role-based training courses from the DHS Information System Security Line of Business and provided these trainings to EXIT users with significant security responsibilities. Management is planning on customizing the role-based training in FY 2015 to reflect the CPSC's policies, procedures, and processes, and to meet the requirements of 5 CFR 930.301.

Issues to be addressed:

- The agency has not updated its Security Training Policies and Procedures since FY 2012. In addition, the Security Training Policy does not require role-based training for non-IT staff, including those non-IT staff explicitly required to receive role-based training in 5 C.F.R 930.301: Executives, Program and Functional Managers, the CIO, and IT functional management.
- The agency does not provide appropriate role-based security training to its personnel. Instead of developing individualized security training for each of the 25 specific user groups outlined in NIST SP 800-16, the agency provides specialized training courses for personnel within the IT department with significant information security responsibilities and a security awareness training for all other CPSC personnel. However, management did not design Role-Based training for non-IT personnel. Also, the Role-Based trainings selected for IT resources with significant security responsibilities do not meet all of the 5 CFR 930.301 required content.

Security Training Recommendations:

1. The agency should update the Security Training Policy and develop a 5 C.F.R 930.301 compliant training program using the guidance outlined in NIST SP 800-16 and NIST SP 800-50.
    a. The Security Awareness and Training policies and procedures should require management to provide each NIST SP 800-16 "user group," defined within the agency security training program, role-based training specifically developed for that group.
    b. The training criteria, if not the content, for each user group should be outlined in the policy. For details on the required training criteria, please see NIST SP 800-16, pages 98−154; NIST SP 800-16, appendix E; and summaries in NIST SP 800-50, pages 25−27.

2. Management should develop/purchase training courses for each of the relevant NIST SP 800-16/NIST SP 800-50, or C.F.R 903.301 user groups, and customize the courses to reflect the CPSC policies, procedures, and processes.

3. Agency management should assign all relevant agency resources to one of the 25 user groups documented in NIST SP 800-16/NIST SP 800-50, or the user groups outlined in C.F.R 903.301.

4. Once management has assigned the users to an agency defined user group, management should then select the appropriate training courses, and provide those security trainings to agency resources commensurate with their user groups.

Remote Access Management

Management has established Remote Access Policies and Procedures. Management also has established the use of Personal Identification Verification (PIV) cards as the common means for the majority of standard users to access the network remotely. In addition, management has implemented the Trusted Internet Connection (TIC) to assist with the government-wide effort to consolidate external network connections across the Federal landscape. The CPSC reports 100 percent of external network/application interconnections and external traffic to/from the organization's networks passes through the TIC in the CIO metrics. However, management allows split tunneling for remote users connecting through the agency VPN, and management operates a router, which does not filter traffic through the TIC. Therefore, does not route 100 percent of its traffic through the TIC, as reported.

Progress:
Management began identifying users who did not authenticate using a PIV card in 2014 to detect and remediate non-compliances with the NIST and HSPD-12 mandates. This new process partially remediates the risk associated with users who remotely access agency systems without multifactor authentication. Management also began performing audits of one form of remote access in FY 2014 to detect unauthorized connections. In addition, management implemented an automated solution to monitor and report on high-risk activity identified by the firewall.

Issues to be addressed:

- The Remote Access policies and procedures are out-of-date and management did not review and update these documents in FY 2014. In addition, these policies and procedures are missing key elements:
    - The policy does not define all authorized methods of remote access.
    - The policy does not include usage restrictions, configuration/connection requirements, and implementation guidance for each remote access method.
    - Management has not documented how they monitor all forms of remote access. In addition, management does not monitor all forms of remote access.
    - Management does not require authorization for remote access, and management permits split tunneling. Also, the policies/procedures do not list the security functions and security-related information that users can access remotely or the additional controls in place to ensure these functions are not misused.
    - Management has not defined the networking protocols the agency has deemed non-secure within the policies/procedures.
- Management has not fully implemented the remote access policies and procedures.
    - The Remote Access policy and Secure Communications policy state that remote sessions time-out after 30 minutes of inactivity. However, management has not configured all remote access sessions to time-out.
    - Management does not monitor all remote connections for unauthorized access or misuse. For example, management does not monitor or review VPN logs as is required by the Remote Access Policy.
    - Management requires the use of FIPS 140-2 in the Secure Communication policy. However, management has not implemented FIPS 140-2 solutions for remote access. Also, management does not systematically require encryption for information

transmitted across public networks, or employ a solution to facilitate the encryption of large file transfers. For example, management has not configured the CPSC email solution to systematically encrypt emails and attachments prior to being transmitted across a public network.
    - Management allows split tunneling and does not require all external network traffic to flow through the TIC.
    - Management permits remote access to all users and, therefore, does not define or document situations or compelling reasons to grant remote access.
    - Management has not reviewed the Remote Access policy since 2012.
    - Management has not developed a traffic flow policy, as required by the System and Communication Protection policy.
- Management does not uniquely identify and authenticate all users and devices accessing the network, including those remotely accessing the network.
    - Management does not require all devices to authenticate to the network, or formally authorize and document a list of devices/types of devices that must authenticate to the network.
    - Management has not implemented a formal process to control the establishment and maintenance of common user accounts, which can be used to remotely access the network.
    - Management does not change common account credentials when users separate from the agency or change job functions.
    - Agency resources use a generic administrator IDs to perform support functions, and management does not monitor the actions performed by these administrator accounts. In addition, agency resources can use these generic administrator IDs to access the network remotely.
- Management did not report all stolen or lost laptops/mobile devices to US-CERT.
- Management does not systematically compel all users to use multifactor authentication to access the network. In addition, multifactor authentication is not used for all forms of remote access.
- Management does not utilize separate accounts for administrators; instead, administrators utilize privileged accounts to perform non-privileged tasks.
- Management lost support for a critical security tool for more than a month in 2014.

Remote Access Management Recommendations:

1. Management should document and implement the following processes in a policy or procedure document:
    a. An inventory of authorized methods of remote access.
    b. Usage restrictions configuration/connection requirements, and implementation guidance for each remote access method.
    c. An inventory of security functions and security-related information that users can access remotely along with the controls management should implement to ensure these functions are not misused.
    d. Specific audit procedures for each remote access method to ensure these controls are in place and effective.
    e. A requirement for management to authorize all forms of remote access prior to allowing this access.

   f. An inventory of networking protocols management deems non-secure and a requirement to restrict access to these protocols.
   g. An inventory of specific and/or types of devices which require unique identification and authentication before establishing a local, remote, and/or network connection.

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

3. Management should configure all remote access sessions to end after 30 minutes in accordance with agency policies and OMB Memorandum M-07-16.

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

5. Management should prohibit split tunneling systematically and route all traffic through the TIC.

6. Management should define, document, and authorize all instances where remote access is granted.

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

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

9. Management should implement a solution that facilitates the encryption of large file transfers.

10. Management should implement a Network Access Control device that requires the Institute of Electrical and Electronics Engineers Standards Association, 802.1x authentication for all CPSC devices (including network devices, servers, and printers) prior to granting access to the network.

11. Management should implement a formal process to establish and control the use of shared user accounts. This should include:
    a. A formal process to approve the creation of new common user accounts.
    b. A formal process to identify and disable common user accounts once these accounts are no longer required.
    c. A formal process to establish membership in the common agency accounts.

d. A formal process to change the common user account's credentials once a member separates from the agency or changes job functions and no longer requires access to the account.
e. A formal process to grant administrators local administrative accounts to each CPSC server individually, instead of using the system administrator accounts. Management should check-in/check-out the global administrative passwords only when this access is required.
f. A formal process that requires management to change the credentials on shared administrator accounts whenever a user with knowledge of these credentials separates from the CPSC or changes job functions.
g. Periodic password changes on all common accounts.
h. A formal periodic review of all common user accounts to ensure these accounts remain appropriate.

12. Management should create separate non-administrative user accounts for administrators, and require administrators to use these accounts when performing tasks that do not require administrative privileges.

13. Management should systematically compel multifactor authentication for all users accessing CPSC systems.

14. Communications between the CPSC management and the U.S. Department of Health and Human Services should improve to eliminate procurement delays associated with critical security solutions. Alternatively, management should consider performing an assessment to determine which procurements are time-sensitive and critical. Once the procurement assessment is complete, management should consider handling those procurements in-house.

15. Management should notify US-CERT and law enforcement of all lost/stolen laptops/mobile devices within the federally and organizationally prescribed timeframes.

16. Management should update the Property Management policies and SOPs to require Property Custodians to notify the ISSO/CSIRT of missing devices that may contain CPSC data (e.g. flash drives, external hard drives, desktops, servers, laptops, Blackberries, etc.) identified throughout the year (e.g. when notified of a lost/stolen device, or as identified as part of the inventory process).

17. Management should train all Property Custodians on their responsibility to notify the ISSO/CSIRT of lost or stolen devices that may contain CPSC data identified throughout the year.

Identity and Access Management

Management has established physical and logical access policies and procedures to govern the Identity and Access Management process. Management also has established the use of PIV cards as the common means for standard users to access agency facilities and log into most agency clients. However, management does not compel users to utilize a PIV card to access all network resources, including privileged accounts.

Progress:
Although management does not require all users to use multifactor authentication to access the network, management has made substantial progress toward that goal, and only a limited number of users exist who can access the network without the use of their PIV Card. Also, in August, management began monitoring the network to identify the users authenticating without a PIV card, and now addresses each of the instances individually. In addition, management also began performing periodic audits of network accounts to identify inappropriate users.

Issues to be addressed:

- Management did not review and update the General Access Control Policy in FY 14. In addition, management did not document the following AC-1 and AC-2 requirements in the General Access Control policy and related procedures:
    - The frequency management reviews/updates the access policies and procedures.
    - The conditions established for role/group membership.
    - A description of the account modification process.
    - The process by which common network accounts are established and controlled, including the process for reissuing shared/group account credentials when individuals are removed from the group.
    - The process by which the organizational personnel responsible for approving privileged access provide additional scrutiny to users being granted privileged access.
    - The process by which temporary, emergency and guest accounts are established and controlled, including the organization-defined duration for each type of account after which the information system is required to automatically remove or disable temporary and emergency accounts.
    - The process by which management controls system accounts.
    - References to individual system access control SOPs.
- Management has not formalized or implemented an Access Control Policy and attendant procedures for all agency applications.
- Management has not fully implemented the General Access Control policy:
    - CPSC ITTS Branch Chiefs and program managers do not assess access controls for all users with administrative and non-administrative access privileges on an annual basis;
        - Management does not audit all users with access to CPSC systems and confirm group access settings are accurate;
        - Management does not maintain a list of all security systems and security controls in place for each system; and,
        - Management does not maintain a description of the processes by which users are granted access to each system.
    - Management utilizes shared administrative accounts.
- Management does not uniquely identify, authenticate, and authorize all users and devices, including those remotely accessing the network, before establishing a connection to the network.

  - o Management does not require all devices to authenticate to the network, or formally authorize and document a list of devices/types of devices that must authenticate to the network.
  - o Management has not implemented a formal process to control the establishment and maintenance of common user accounts, including those which can be used to remotely access the network.
  - o Management does not change common account credentials when users separate from the agency or change job functions.
  - o Agency resources use a generic administrator IDs to perform support functions, and management does not monitor the actions performed by these administrator accounts. In addition, agency resources can use these generic administrator IDs to access the network remotely.
- – As also mentioned in the Remote Access Section, system administrators do not utilize separate user accounts when performing non-administrative tasks.
- – The agency has not implemented the Principle of Least Privilege and the proper separation of duties for the GSS LAN.
- – Management has not implemented the Principle of Least Privilege or Segregation of Duties within www.cpsc.gov.
- – Management did not revoke access to agency information systems immediately upon contractor/employee separation from the agency. Also, management does not document and maintain the time and date the agency revokes network accounts. Therefore, management cannot evidence the timeliness of these access revocations.
- – Management has not defined a process to establish common accounts, periodically review common accounts, or to change the passwords for these accounts as business needs require.
- – As mentioned in the Remote Access Section, management does not systematically compel all users to use multifactor authentication to access the network. In addition, multifactor authentication is not used for all forms of privileged and remote access.

Identity and Access Management Recommendations:

1. Management should review and update the General Access Control policy annually.

2. The following elements should be included in the General Access Control Policy and procedure documents:
   a. The frequency management reviews/updates the access policies and procedures.
   b. The process by which management establishes and controls temporary, emergency, and guest accounts. This should include guidance on how guest/temporary accounts are authorized and monitored. Management should also define a process for notifying account managers when temporary accounts are no longer required, in addition to the requirement to deactivate temporary accounts that are no longer required. Also, management should codify the organization-defined duration for each type of account after which the information system is required to automatically remove or; disable temporary and emergency accounts.
   c. Specific procedures for the establishment and modification of user accounts, including a requirement for all new administrators to follow the formal user access request process.

d. The process by which common network accounts are established and controlled. This should include how common/anonymous accounts are authorized and monitored and how shared credentials are reissued when individuals are removed from the group.
e. The process by which management authorizes privileged access. This should include a description of the additional scrutiny the authorizing resources apply to the authorization of privileged access. This should also include a list or description of the appropriate authorizing resources (e.g. system owner, mission/business owner, or Authorizing Official).
f. The process by which the agency establishes and controls system accounts.
g. Individual system access control SOPs should be referenced in the General Access policy.

3. Management should draft, approve, and implement NIST compliant Access Control policies and procedures for agency applications.

4. Management should ensure that the General Access Control Policy is fully implemented. This includes requiring that the ITTS Branch Chiefs and program managers assess access controls for all users with administrative and non-administrative access privileges on an annual basis:
   a. Management should maintain documentation to include a list of all security systems and security controls in place for each system.
   b. Management should maintain an up-to-date list of the process by which users are granted to each system.
   c. Management should audit all users with access to CPSC systems and confirm group access settings are accurate.
   d. Management should not utilize shared administrator accounts.
   e. Management should ensure that all Access Control policies and procedures are disseminated to all resources with significant access control roles and responsibilities.

5. Management should implement the Principle of Least Privilege for the GSS LAN.
   a. The agency should define and document the functions/duties which have a significant impact on agency operations and assets (e.g. create users accounts, modify firewall rules, modify antivirus settings, reset passwords, modify DHCP, etc.) and create roles that systematically separate the users' ability to perform these functions.
   b. The agency should revoke access to all users who have but do not require access to the functions defined above.
   c. The agency should review the logs of all admin/super user accounts and restrict this access if these levels of privilege are not specifically necessary to perform required job functions.
   d. The agency should document the system controls in place (e.g. blocked ports, restricted protocols, etc.).
   e. The agency should document the specific access controls in place for providing/controlling access required for the duties, functions and system restrictions described above. Documentation can be in the form of access control policies (e.g. identity-based policies, role-based policies, attribute-based policies, etc.).

f. Management should create separate non-administrative user accounts for administrators and require administrators to use these accounts when performing tasks that do not require administrative privileges.

6. Management should implement a solution that allows the agency to report on the specific privileges assigned to each Active Directory and e-Directory user account. These reports should be granular enough to report on which security function management assigns to each user account. Management should perform periodic audits of these reports to ensure access remains appropriate.

7. Management should limit administrator's access to update audit logs and implement a solution to monitor changes to the audit logs and notify the CSIRT team in the event of an audit log modification.

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

9. Management should develop and implement workflows within cpsc.gov to coincide with the roles defined within www.cpsc.gov.

10. Management should revoke separated users' access to agency systems.

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

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

13. Management should train the Contracting Officers Representatives, EXRM, and EXIT resources responsible for processing contractor separations on their respective contractor separation responsibilities.

14. EXRM should provide the EXIT representatives and program officials responsible for processing contractor separations with a weekly report of contractor separations. Management should formally reconcile the current separations, as indicated on the weekly EXRM contractor separation report, to all the CPSC IT system Access Control Lists to ensure the timely revocation of all user accounts.

15. Management should periodically review all user accounts to ensure that access remains appropriate.

16. Management should implement a process to establish and control the use of shared user accounts.

a. Management should implement a formal process to approve the creation of new common user accounts.
b. Management should implement a formal process to disable common user accounts once no longer required.
c. Management should implement a formal process to establish membership in the common agency accounts.
d. Management should implement a formal process to change the common user account's credentials once a member separates from the agency or changes job functions and no longer requires access to the account.
e. Management should grant administrators local administrative accounts to each CPSC server individually, instead of using the system administrator accounts. Management should check-in/check-out the passwords to the global system administrator accounts only when this access is required.
f. Management should implement a formal process to require management to change the credentials on shared administrator accounts whenever a user with knowledge of these credentials separates from the CPSC or changes job functions.
g. Management should require periodic password changes on all common accounts.
h. Management should require a formal periodic review of all common user accounts to ensure these accounts remain appropriate.

17. Management should systematically require all users accessing the CPSC network to use multifactor authentication.

APPENDIX A: MANAGEMENT RESPONSE

PAGE INTENTIONALLY LEFT BLANK

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

Memorandum

Date: November 7, 2014

TO : Christopher Dentel
Inspector General
Office of the Inspector General

THROUGH: Patrick Manley
Information Systems Security Officer
Office of Information Technology (EXIT)

FROM : Pat Weddle MJ for Pat Weddle
Chief Information Officer
Office of Information Technology (EXIT)

SUBJECT : Management Response to FY 2014 Evaluation of the CPSC's Federal Information Security Management Act (FISMA) Implementation

Thank you for the opportunity to respond to the FY 2014 FISMA evaluation. The Office of Information Technology (EXIT) has continued to make progress in its IT security program over the past year. An Incident Response Team, with dedicated resources, was established to help the agency identify and thwart cyber-attacks aimed at compromising the agency's information systems and data; and EXIT began a project to assess the information systems being utilized by staff at the National Product Testing and Evaluation Center (NPTEC). In response to an OMB mandate issued last fall, requiring all Federal agencies to implement strategies to more efficiently monitor information system security controls, EXIT developed associated policies, risk assessments and monitoring plans needed to comply with this mandate. EXIT has also procured a governance, risk and compliance tool which will allow the office to better manage security documentation, such as security plans, assessments, and policies.

EXIT has carefully reviewed the evaluation and generally concurs with its findings. There are two areas EXIT would like to highlight:

Risk Profile of Findings

The evaluation does not address the risk profile associated with findings and whether a particular finding induces a quantifiable weakness or vulnerability within agency information systems. OMB Circular A-130, which establishes official OMB policy and guidance on information technology management for Federal executive agencies, requires that agencies utilize the concept of "adequate security" when employing security controls. Adequate security is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition emphasizes a risk-based policy for cost-effective security established by the

Computer Security Act. In the *Risk Management Review* section of the evaluation, there is a finding related to EXIT not performing an assessment of security controls employed by minor applications (pg. 7). The agency employs approximately 80 different minor applications—ranging from document tracking systems to macro-based spreadsheets. The overwhelming majority of the security controls employed by minor applications are directly inherited from the general support network, on which most of these systems reside. The time and cost associated with a formal security review of each of these applications would be substantial and would not significantly alter the agency's risk exposure. It is conceivable that by diverting resources to address these types of findings, the agency could be creating "increased" risk for its systems and data. Findings that identify more serious and immediate vulnerabilities would necessarily have to compete with "risk-neutral" findings for limited IT security resources.

Cost-Benefit of Remediation

The evaluation does not discuss the cost-benefit ratio associated with remediation activity and whether addressing a particular finding would be appropriate. In the *Security Training* section, the evaluation states a deficiency regarding the agency's failure to provide appropriate role-based security training (pg. 23).

As mandated by FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, Federal agencies are required to apply an appropriately tailored set of baseline security controls as specified in National Institute for Standards and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST 800-53 only requires agencies to provide role-based security training to personnel with *assigned security roles and responsibilities*. The time and cost associated with the development, maintenance and delivery of security training for 25 distinct user groups would be substantial and would not significantly alter the agency's risk exposure. Implementing the evaluation's recommendation would exceed the NIST 800-53 requirement.

EXIT acknowledges that there are relevant security weaknesses identified in the FY 2014 FISMA evaluation. EXIT will prepare a remediation plan to address the issues that create a measurable level of risk to CPSC's information systems and which are balanced by the effect of implementing the CAP goals. These weaknesses will be documented in EXIT's Plan of Action and Milestones (POAM) tracking system.