

U.S CONSUMER PRODUCT SAFETY COMMISSION



OFFICE OF THE INSPECTOR GENERAL

CONSUMER PRODCUT SAFETY RISK
MANAGEMENT SYSTEM
INFORMATION SECURITY REVIEW
REPORT

Fieldwork: December 2010 to February 2011

Issued: June 4, 2012



UNITED STATES
CONSUMER PRODUCT SAFETY COMMISSION
BETHESDA, MD 20814

Memorandum

Date: June 5, 2012

TO : Inez Tenenbaum
Chairman

FROM : Christopher W. Dentel
Inspector General

SUBJECT : Security Review of the CPSC's Consumer Product Safety Risk Management System

The Office of Inspector General has completed its security review of the CPSC's Consumer Product Safety Risk Management System. A copy of the resulting report is attached.

Management (EXIT and OEX) has been briefed regarding the findings and recommendations of this audit and given an opportunity to respond to them. Management's response may be found as an attachment to the audit report. Management generally concurred with the findings of the audit and either agreed to implement corrective actions regarding those findings or indicated that corrective action had already been taken.

If you have any questions about this report or wish to discuss it, please feel free to contact me at 301-504-7644 or cdentel@cpsc.gov.



Christopher W. Dentel
Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
BACKGROUND	3
OBJECTIVE	3
SUMMARY OF FINDINGS	4
RECOMMENDATIONS	4
AUDITEE COMMENTS.....	6
INTRODUCTION	7
OBJECTIVE, SCOPE & METHODOLOGY.....	8
OBJECTIVE	8
SCOPE	8
METHODOLOGY	9
RESULTS OF EVALUATION	11
SUMMARY	11
FINDINGS AND RECOMMEDATIONS	11
FINDING 1: The draft Risk Management Framework strategy has yet to be formalized or implemented.	11
FINDING 2: The CPSC has not yet developed an Enterprise Architecture with Information Security considerations.	12
FINDING 3: Insufficient documentation of the implementation of NIST SP 800-53 security controls in the CPSRMS SSP.....	13
FINDING 4: The CPSRMS SSP does not reflect the most current information and often contradicts other Security control documents.....	15
FINDING 5: The CPSRMS POAM does not include all elements required by OMB Memorandum 04-25.....	17
FINDING 6: The CPSRMS Security Categorization Document does not adequately justify impact assignments for 10 of the identified information types.	18
FINDING 7: Insufficient documentation of the analysis disqualifying the non-selected information types in the CPSRMS Security Categorization Document.	21
FINDING 8: The CPSRMS SSP does not outline specific Public Access controls in place to mitigate the risks associated with allowing external user’s access to CPSRMS.	21
APPENDIX I: MANGEMENT RESPONSE	23

EXECUTIVE SUMMARY

BACKGROUND

The Consumer Product Safety Improvement Act of 2008 (CPSIA), P.L. 110-314, Section 212 requires the Consumer Product Safety Commission (CPSC) to implement a publicly accessible, searchable database of consumer product incident reports. To meet this requirement the CPSC developed the Consumer Product Safety Risk Management System (CPSRMS). The CPSRMS houses personal, proprietary, and confidential data. As defined by NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, CPSRMS is categorized as a major application. Therefore, CPSRMS is required to implement specific security controls and complete a Security Certification and Accreditation (C&A) separate from the CPSC General Support System (GSS LAN). NIST SP 800-37, *Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010 provides guidance and best practices for the C&A process that agencies are required to implement as a mandate of the Federal Information Security Management Act (FISMA). Consequently, CPSC management has reviewed and validated CPSRMS's system security through the performance of a C&A assessment and formally authorized CPSRMS to operate on January 16, 2011.

To satisfy the NIST SP 800-37 requirements, the CPSC contracted with Communications Resources Inc. (CRI), an outside IT consultancy to perform the initial categorization, selection, and implementation of the CPSRMS security controls, and to develop the CPSRMS System Security Plan (SSP). Other deliverables provided by CRI included:

- CPSRMS Risk Assessment
- CPSRMS Security Categorization Document
- CPSRMS Security Control Implementation Plan (SCIP)
- CPSC Business Impact Analysis (BIA)

CPSC also contracted with SecureIT, whom is responsible for developing the GSS LAN SSP and GSS LAN Security Assessment Report (SAR), to perform an independent security assessment of the CPSRMS implementation and develop the SAR for CPSRMS. SecureIT would also be responsible for maintaining the CPSRMS SSP and be responsible for developing the Continuous Monitoring Plan and the Asset Inventory Report.

OBJECTIVE

As required by Section 205(a)(1) of the Consumer Product Safety Improvement Act (CPSIA) of 2008, the Office of Inspector General (OIG) is required to conduct reviews and audits to assess the CPSC's information technology architecture and systems and the development of the public database. In order to determine if the availability, confidentiality, and integrity of data housed in CPSRMS is adequate, agency officials must perform a C&A on the system. As such, the objective of this evaluation was to

review the application of the Risk Management Framework, as defined in NIST 800-37, to the CPSC's implementation of the CPRMS.

SUMMARY OF FINDINGS

At the time fieldwork was performed (December 2010 through February 2011), there were several inconsistencies and weaknesses in the C&A assessment of the CPRMS. These weaknesses stemmed primarily from a lack of mature organizational processes and procedural documents required to ensure the adequate governance of the C&A process. In addition, management's lack of internal resources played a significant part in the weaknesses identified in the C&A assessment. Our findings include the following:

1. The draft Risk Management Framework strategy has yet to be formalized or implemented.
2. The CPSC has not yet developed an Enterprise Architecture with Information Security considerations.
3. There is insufficient documentation of the implementation of NIST SP 800-53, *Revision 3 Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009, security controls in the CPRMS SSP.
4. The CPRMS SSP does not reflect the most current information and often contradicts other Security control documents.
5. The CPRMS Plan of Action and Milestones (POAM) does not include all elements, required by Office of Management and Budget (OMB) Memoranda 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, dated August 23, 2004.
6. The CPRMS Security Categorization Document does not adequately justify impact assignments for 10 of the identified information types.
7. There is insufficient documentation of the analysis disqualifying the non-selected information types in the CPRMS Security Categorization Document.
8. The CPRMS SSP does not outline specific Public Access controls in place to mitigate the risks associated with allowing external user's access to CPRMS.

RECOMMENDATIONS

Once CPSC addresses the aforementioned issues, many of the subsequent C&A tasks will become significantly less cumbersome to administer, and the process will become more controlled and transparent. To assist the CPSC in addressing the weaknesses identified above, we are providing the following recommendations:

1. Identify the participants of the CPSC Risk Executive Council and define specific tasks/milestones for implementing the proposed Risk Management Framework. CPSC Senior Management should then define a methodology for developing and establishing a formal organizational tolerance for risk in the Risk Management Framework.
2. Develop an Enterprise Architecture that includes a comprehensive IT Security Architecture using the CIO Counsel's guidance (FEA-Security-Privacy-Profile-v3-9-30-2010) and incorporate this into the Security Control Documents. Further, all the security controls, including the NIST SP 800-53 required controls, should be mapped to the Enterprise Architecture/Information Security Architecture to provide a comprehensive view of the security control relationships.
3. Fully document the implementation of the security controls, including the implementation of the sub-controls, in the CPSRMS SSP with sufficient detail to facilitate the assessment of individual controls.
4. Update the CPSRMS SSP to be the single authoritative system security document. The update of the document should include the correct go-live date and the latest understanding of the current state of CPSRMS Security. As such, the CPSC should:
 - a. Revise and update the CPSRMS SSP and the other security control documents to identify and reconcile all inconsistencies between said documents.
 - b. Management should perform an assessment over the independent contractor control assessments to determine which position the CPSC will support. Upon completion of the assessment, the CPSRMS SSP should document CPSC's current position in addition to the justification for any positions held in opposition to SecureIT.
 - c. Update the CPSRMS SSP to include the results of other technical security reviews.
 - d. Reassess the common, hybrid, and system specific control significations to provide accurate descriptions of controls in the CPSRMS SSP.
 - e. Re-scan the network to define all devices with the CPSRMS System Boundary. Document the results of this scan in the SSP.
5. Update the POAM to include the missing information, as required by OMB M-4-25.
6. Perform an assessment to ensure the adequate categorization of Information Types. The logic for categorizing the Information Types as "High", "Moderate", or "Low" should be consistent with the guidance provided in NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*, dated August 2008.
7. An analysis should be performed to ensure that all of the Information Types outlined in the NIST 800-60 framework were appropriately included in or excluded from the CPSRMS Security Categorization document.

8. Define the specific Public Access controls in place/planned, or reference the document defining these controls within the CPSRMS SSP.

AUDITEE COMMENTS

The auditee responses have been included as an appendix to this report. The auditees concurred with the majority of our findings and recommendations and indicated that work has been completed or is already in progress to address many of the deficiencies found.

INTRODUCTION

The Consumer Product Safety Commission Public Database

The Consumer Product Safety Improvement Act of 2008 (CPSIA), P.L. 110-314, Section 212 requires the CPSC to implement a publicly accessible, searchable database of consumer product incident reports. Pursuant to section 6A(a)(3) of the CPSIA, the database must be established within the 18-month period following the CPSC's submission of a plan to Congress regarding the Database implementation under section 6A(a)(2). The CPSC submitted this plan to Congress on September 10, 2009. Therefore, the Database launch date was set for March 11, 2011.

The Consumer Product Safety Risk Management System

The CPSC contracted with InfoReliance (IR) on August 18, 2008, to begin the development of a solution to meet this legislative requirement for a public database. IR customized one of its Commercial-Off-The-Shelf (COTS) products to meet the requirements defined by the CPSIA/CPSC management and developed SaferProducts.gov. The purpose of this tool is to provide a single, central location where consumers can report incidents and search for prior incidents/recalls. Additionally, this tool will provide the manufacturers of the products in question with an opportunity to comment on actions taken to remediate the product safety concerns, as well as rebut, correct, and add additional precision to such reports. Moreover, this tool is an integral part of the overall IT Modernization effort, termed CPSRMS. As such, it is the expectation of the CPSC that the implementation of CPSRMS is to occur over the course of the next 2 to 3 years at the CPSC.

The CPSRMS architecture includes a core development framework, in addition to, three key applications using the framework: Consumer/Public Portal, Industry Partner Portal, and Incident Management Control Center (IMCC). By customizing an existing COTS product, the CPSC does not have to develop and support an in-house solution and has the option to draw from an outside pool of experts for future support needs. However, the challenge with this type of implementation is integrating the COTS tool with the legacy solutions already in place at the CPSC. Therefore, in order to ensure the validity of the IR architectural documentation and identify security vulnerabilities associated with the overall CPSRMS architecture, which includes the integration between the IR solution and the legacy systems already in place, the CPSC contracted with Aspect Security on June 29, 2010, to perform an independent architectural security review. The scope of this review included the custom application components and related controls developed by the CPSC. Analysis of these custom application components and controls focused on the areas of Identity Management and Authentication, Session Management, Access Control, Input Validation and Output Encoding, and Sensitive Data Protection.

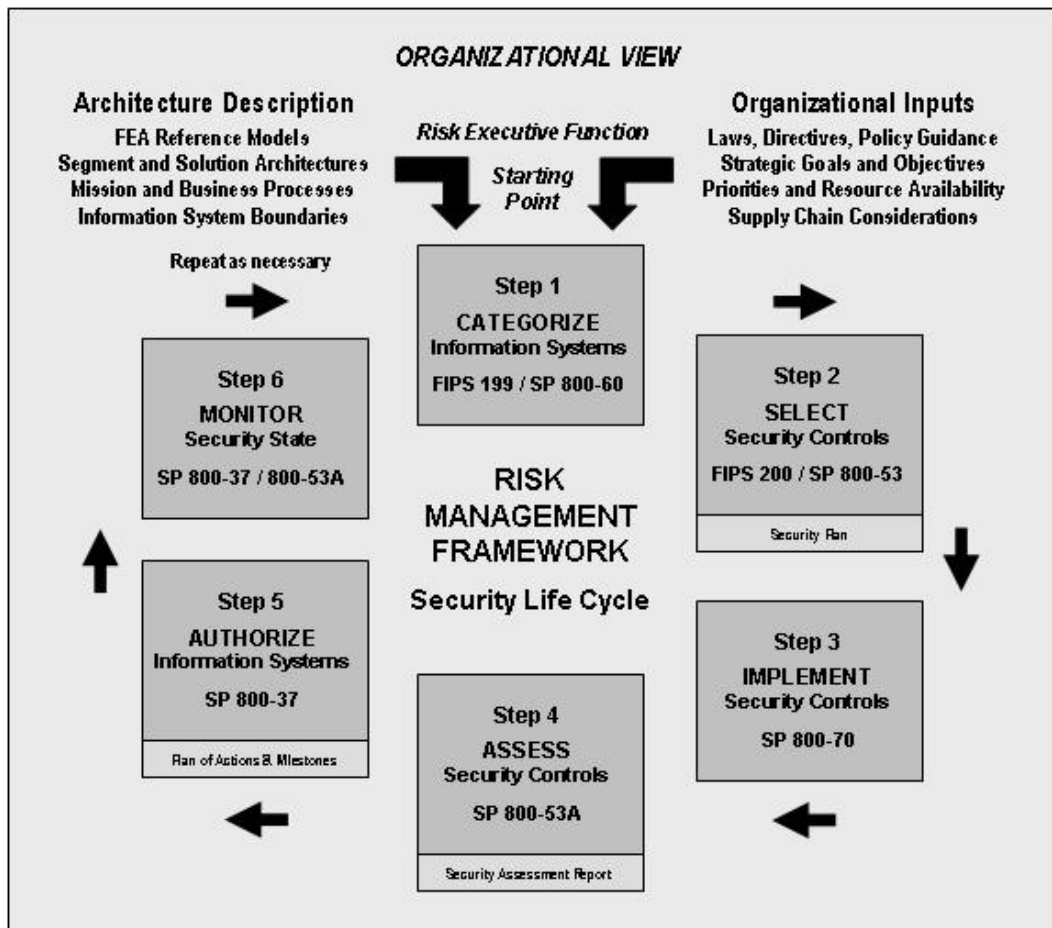
OBJECTIVE, SCOPE & METHODOLOGY

OBJECTIVE

The objective of this review was to assess the application of the Risk Management Framework, as defined in NIST 800-37, to the CPRMS implementation. This was to ensure the agency performed all of the tasks required to ensure the availability, confidentiality and integrity of the data housed in CPRMS.

SCOPE

This evaluation consisted of review of CPSC’s C&A assessment of CPRMS against the Risk Management Framework, as outlined in NIST SP 800-37, *Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010 and the requirements of Section 212 of the CPSIA. As such, our review included the following processes within the boundaries of the CPRMS solution:



METHODOLOGY

This review is not an audit, thus it was not conducted in accordance with generally accepted government auditing standards. As such, our review was conducted in accordance with Quality Standards for Inspections and Review. The performance of fieldwork occurred from December 2010 to February 2011 at the CPSC's headquarters located in Bethesda, Maryland. In order to accomplish our objective, we reviewed the requirements of the CPSRMS implementation through obtaining and reviewing the key reports developed by CPSC management and their independent contractors, documenting the CPSRMS implementation and related security architecture. Throughout our review of supporting documents obtained, we held key discussions with the Office of Information and Technology's (EXIT) Chief Information Officer, Division of Policy and Planning (ITPP) Director, Information Systems Security Officer, and relevant members of their staffs.

The principle criteria used for this review included:

- The Consumer Product Safety Improvement Act of 2008, P.L. 110-314, Section 212
- Federal Information Security Management Act of 2003, Title III of the E-Government Act of 2002, P.L. 107-347
- OMB Circular A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, dated November 28, 2000
- OMB Memoranda 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, dated August 23, 2004
- NIST SP 800-37, *Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010
- NIST SP 800-39 (Draft), *Managing Information Security Risk: Organization, Mission, and Information System View*, dated March 2011
- NIST SP 800-53, *Revision 3 Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009
- NIST SP 800-53A, *Revision 1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, dated June 2010
- NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2:*

Appendices, dated August 2008

- NIST SP 800-70, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, February 2011
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006

RESULTS OF EVALUATION

SUMMARY

Overall, we found several inconsistencies and weaknesses in the way the CPSC executed the C&A process of CPSRMS. These weaknesses stemmed primarily from a lack of organizational resources at the time of CPSRMS implementation; thus, resulting in the heavy reliance on independent contractors for the development and implementation of CPSRMS. Further, the lack of mature organizational processes and procedural documents required to ensure the adequate governance of the C&A process also contributed to the inconsistencies and weaknesses found.

FINDINGS AND RECOMMENDATIONS

FINDING 1: The draft Risk Management Framework strategy has yet to be formalized or implemented.

A Risk Management Framework has been drafted, but not been implemented. As such, the CPSC has not formally implemented a Risk Executive (function). The CPSC Security team documented the CPSC Risk Management Framework based on the NIST SP 800-39 (Draft), *Managing Information Security Risk: Organization, Mission, and Information System View*, dated April 2008. NIST SP 800-39 outlined the proposed approach to addressing risk from an organizational perspective and it addresses most of the NIST SP 800-37 requirements. The implementation of Risk Management Framework and the establishment Risk Executive (function) did not occur due to a lack of resources available to perform the required duties and a lack of management support for the creation of these organizational roles. Consequently, the tasks required in NIST SP 800-37 and NIST SP 800-39 are not being performed. Thus, there is a strong likelihood that the agency has not assigned the correct amount of effort/ resources to identifying, prioritizing, and mitigating agency risks.

Moreover, the CPSC did not document one of the topics that NIST SP 800-37 requires in the Risk Management strategy – the Organizational Risk Tolerance. Per CPSC management, the Organizational Risk Tolerance has not been defined or documented. For C&A purposes, CPSC management informally tied the Agency Organizational Risk Tolerance to the CPSRMS system categorization of “Moderate.” The system categorization of “Moderate” was defined using FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004. Management also documented the level of risk acceptable for CPSRMS to operate in the Authorization to Operate (ATO) document. The ATO document states that CPSRMS will not be authorized to operate if any “high-impact” security weaknesses are identified and unmitigated. The CPSRMS POAM listing is where security weaknesses are documented and assigned impact levels. This listing is derived from several assessments, including the CPSRMS SSP, SAR, and various technical evaluations.

Recommendations:

1. Identify the participants in the CPSC Risk Executive Council, and then begin the top-down and bottom-up process of developing a risk management organization. A top down approach to developing a risk management organization requires senior management to identify the participants of the Executive Risk Council. A bottom up approach to developing the risk management organization requires the Executive Risk Council to identify the resources responsible to provide the relevant risk information within the organization. Additionally, require these resources, as outlined in the Risk Management Framework, to begin taking on the risk management responsibilities assigned to them.
2. Define specific tasks and milestones associated with implementing the proposed Risk Management Framework. Additionally, implement a process to track and quantify the aggregate risks from all Information Systems (*e.g.*, a risk heat map) and include this procedure in the Risk Management Framework. This should be lead by the Risk Executive Function and tied to the Enterprise Architecture.
3. Senior CPSC management (*e.g.*, the Risk Executive Function) should define a methodology for developing the risk tolerance for the CPSC and formally establish an organizational tolerance for risk in the Risk Management Framework. The risk tolerance should be communicated and guidance provided to appropriate agency resources on how risk tolerance impacts ongoing decision making activities, as recommended by NIST SP 800-39 (Draft). Moreover, update the Risk Assessment to include documentation of the risk tolerance and used to justify the ATO decisions going forward.

FINDING 2: The CPSC has not yet developed an Enterprise Architecture with Information Security considerations.

The CPSC has not yet developed an Enterprise Architecture with Information Security considerations; therefore, the information types and security controls have never been mapped to the Enterprise Architecture. This is due to the amount of effort required to document the Enterprise Architecture and the limited number of agency resources assigned to this effort. This has lead to the CPSC's inability to document properly the implementation of system-specific and hybrid security controls within the information system while taking into account specific technologies and platform dependencies. Additionally, the CPSRMS SSP states that the Information Security and Enterprise Architecture was planned to be implemented for FY 2010; however, that deadline has passed, and this had not yet been accomplished. Without a comprehensive Enterprise Architecture, entire enterprise components (Segment and Solution Architectures) may go unidentified, and the weaknesses associated with these enterprise components may go unremediated due to this lack of mapping and visibility.

Recommendations:

Develop an Enterprise Architecture that includes a comprehensive IT Security Architecture using the CIO Counsel's guidance (FEA-Security-Privacy-Profile-v3-9-30-2010) and incorporate this into the relevant Security Control Documents. Additionally, all the security controls, including the controls required by NIST SP 800-53, *Revision 3 Recommended Security Controls for Federal Information Systems and Organizations*, dated August 2009, should be mapped to the Enterprise Architecture/Information Security Architecture to provide a comprehensive view of the security control relationships. CPSC can accomplish this through the development of Segment Architectures based on the primary CPSC mission objectives and business processes. Once the definition of segments occurs, a Solution Architecture should be designed for each of the individual Segments. The Solution Architectures should include details that define each of the related security controls, including those defined in NIST SP 800-53. The Solution Architecture should also include mapping to the other Solution and Segment Architectures and with this view, controls should be classified as "Common," "Hybrid," or "System Specific." For controls defined as "Hybrid," these controls should be included in all associated Solution/Segment Architectures to ensure that the control components are properly mapped to each of the participating systems. As for all controls defined as "Common," these controls should be included (or referred to) in each of the associated Solution/Segment Architectures to provide a full view of the security of each of the Solutions and Segment Architectures. In addition, to assign priority and criticality to each of the IT Systems in terms of "Confidentiality," "Integrity," and "Availability," the use of Enterprise Architecture is appropriate, and this process is not defined in any of the other Security Control Documents.

To assist management in categorizing Information Types and their associated Information Systems in terms of their impact on Confidentiality, Availability, and Integrity, the use of the Enterprise Architecture is appropriate. The Information Types should be defined in the Information Catalog section of the Business Architecture. Additionally, a section in this catalog should be included to categorize this impact in both mission continuity terms and NIST terms as these two views differ, but they are both important to management from a planning and control perspective.

FINDING 3: Insufficient documentation of the implementation of NIST SP 800-53 security controls in the CPSRMS SSP.

The implementation of the NIST SP 800-53 security controls did not include sufficient detail of implementation in the CPSRMS SSP. This was due to lack of management oversight of the CRI contract and management not effectively enforcing the stipulations set forth in the CRI Statement of Work. Without sufficient detail, the traceability to the decisions made prior to and after the deployment of the information system, as required by NIST SP 800-37, may not be possible. As such, we noted the following:

- a) Individual documentation of the sub-controls and their implementation was not included; therefore, the CPSRMS SSP was unable to describe “*the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control.*” Moreover, the control developer/implementer did not provide a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control, as required by NIST 800-53. The implementation description included a description of the finding, if the control was deemed to be not fully compliant, or a high-level description of the control, if it was deemed to be in place; however, the control descriptions were not defined in terms of “Planned Inputs,” “Expected Behavior,” and “Expected Outputs,” as required. Further, it was noted that a description that might be used to document “Minimum Assurance Requirements” was not documented. Although the SCIP documented unimplemented controls in these terms, it contains only 12 security controls. However, there were 86 “Planned,” “Partially Compliant,” or “Noncompliant” controls that appeared in the SSP and 47 “Other than Satisfied” controls that appeared in the CPSRMS SAR. Additionally, the CPSRMS SARs did not include sufficient descriptions of any of the controls considered fully implemented.
- b) Four controls: PM-10, SI-10, AU-9, and IA-8, were defined, as “Partially Compliant” in the CPSRMS SSP, but did not have an associated implementation strategy documented in the CPSRMS SSP; and were not separately documented in the SCIP or Risk Assessment. Instead, where this information should have been documented, the signification “None” appeared.
- c) The documentation regarding tailoring of the baseline security controls, by applying scoping, parameterization, and compensating control guidance, was incomplete. For example, parameterization details such as configuration parameters; session timeout; registry settings; account, file, and directory settings (*i.e.* permissions, and settings for services, ports, protocols, and remote connections) were not documented in the CPSRMS SSP. In addition, guidance on how the agency plans to employ compensating controls was not documented in the CPSRMS SSP.
- d) The documentation for the justification for adding 10 supplemental controls to the CPSRMS SSP was incomplete. As NIST SP 800-53 provisions for a moderate impact system did not require these controls, OMB A-130 states that the agency must “*Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications.*”

Recommendations:

1. Fully document the implementation of the security controls, including the implementation of the sub-controls, in the CPSRMS SSP with sufficient detail to

facilitate the assessment of individual controls. This includes documenting specific actions that will be required to perform the control, as well as determining whether to accept that the control is correctly designed and operating effectively by defining the Minimum Assurance Requirements. The CPRMS SAR format is a more effective format to accomplish this than the one currently being used for the CPRMS SSP.

2. Define all security controls assessed in the CPRMS SSP/SAR assessments in terms of “Planned Inputs” (including cost and resources required), “Expected Behavior,” and “Expected Outputs” within the CPRMS SSP, SCIP, or Risk Assessment. If this is not to be documented directly in the text of the CPRMS SSP, then the document that has this information should be included as an Appendix in the CPRMS SSP to provide adequate traceability for decisions made prior to and after the implementation of CPRMS.
3. Document the cost-benefit analysis for adding each of the supplemental NIST SP 800-53 controls. Additional explanatory details should be added to the CPRMS SSP to justify the additional 10 controls.
4. Add control parameters to the control descriptions in the SSP, where applicable.
5. Draft an implementation plan for each of the CPRMS security controls, as well as for the four “Planned” controls identified without a planned implementation strategy (PM-10, SI-10, AU-9, and IA-8). The CPRMS SSP should document the planned implementation strategy. This may be accomplished by updating the SCIP to include all controls identified in the CPRMS SSP and CPRMS SAR as “Other than Satisfied,” “Planned,” “Partially Compliant,” or “Noncompliant.”
6. All controls that were considered “Other than Satisfied,” “Planned,” “Partially Compliant,” or “Noncompliant” as per the SSP or SAR should be included on the POAM or have the justification for their exclusion from the POAM documented.

FINDING 4: The CPRMS SSP does not reflect the most current information and often contradicts other Security control documents.

The CPRMS SSP does not reflect the most current information and often contradicts other Security control documents. The disagreement and inconsistencies amongst the security control documents was attributed to management’s inability to establish a methodology to reconcile the divergence in the reporting styles of the two vendors, who performed and documented the assessments. For example, each vendor used different criteria to define “Common,” “Hybrid” and “System Specific” controls, as well as used different criteria to assess the compliance of the required NIST controls. Management did not know of the differences until notification by the OIG. Consequently, this has led to an incomplete/inaccurate representation of the CPRMS security profile and a general lack of consistency between the security control documents. For example, we noted the

following:

- a) The CPSRMS SSP states that CPSRMS “will be operational in October 2010” and the launch at the time of fieldwork was set for March 11, 2011.
- b) Twenty devices identified in the CPSRMS system boundary as part of the SecureIT Inventory Assessment were not included in the CPSRMS SSP.
- c) The CPSRMS SSP does not include the vulnerabilities identified as part of the Security Assessment Report and other technical assessments (*e.g.*, assessments performed by Aspect Security)
- d) The CPSRMS SSP, developed by CRI, does not define “Common” controls the same way as Secure IT's developed CPSRMS SAR or the GSS LAN. There are 17 System Specific/Hybrid controls assessed and defined in the SSP by SecureIT, as part of their independent validation of the implementation of NIST SP 800-53 security controls, and documented in the CPSRMS SAR as “System Specific” or “Hybrid” controls. Instead, these controls were defined as “Common” and were tested and documented as part of the GSS LAN SAR.
- e) SecureIT’s original assessment of SC-14 was “Not Compliant,” which was documented (although never subsequently updated after its reassessment) in the GSS LAN SSP. Then, after some remediation, SC-14 was reassessed as part of the CPSRMS SAR process and it was deemed “In Place,” which is the position that management holds. However, CRI holds a different position and considers this control to be “Partially Compliant,” as is documented in the CPSRMS SSP, even after the control reassessment. Furthermore, management has not documented which position it supports along with their justification for holding this position.
- f) Three controls: SI-03, SC-02, and SC-23, which were identified on the SAR as “Satisfied” were identified on the SCIP, either as “Planned,” or “Solution Identified” but not implemented. Moreover, the CPSRMS SSP identified these three controls as either “Noncompliant” (SI -03) or “Partially Compliant” (SC-02 and SC-23).

Recommendations:

1. Update the SSP to include the correct go-live date and to reflect the latest understanding of the current state of CPSRMS security. As such, CPSC should perform the following:
 - a. Reconcile the CPSRMS SSP with the other security control documents (*e.g.*, CPSRMS SAR, GSS LAN SAR, SCIP, Security Categorization Document, and Risk Assessments), to identify all variances and update the documents to

present one consistent “snapshot” of system security.

- b. Management should also perform an assessment to determine which position it supports (with significant weight given to the independent assessors) and justify/document their position in the SSP so that the SSP can be the single, authoritative security document for CPSRMS.
 - c. Additionally, to support the objective of the CPSRMS SSP becoming the single, authoritative security document for CPSRMS, updates to the SSP should include the results of the related SARs and other technical security reviews (*e.g.*, Aspect Security reviews).
 - d. Reassess the “Common,” “Hybrid,” and “System Specific” control significations, and update the SSP to include an accurate description of controls in addition to the justification for each of the control significations.
 - e. The network should be re-scanned to define all of the devices within the CPSRMS System Boundary and the results of this scan should be included in the SSP. Moreover, management should reassess any additional controls required because of the discoveries made by this scan for proper implementation and document the results of this assessment in the SSP, if applicable.
2. A description of how CPSRMS is integrated into the Enterprise Architecture, which should include the Information Security Architecture, should be documented in the CPSRMS SSP.
 3. Update the POAM to reflect the changes made to the updated SSP, where applicable.

FINDING 5: The CPSRMS POAM does not include all elements required by OMB Memorandum 04-25.

The POAM does not include all OMB M-4-25 required components. It was noted that the CPSC’s POAM process is in an immature state; thus, resulting in incomplete implementation. With incomplete implementation of the POAM, vulnerabilities may not be properly tracked and reported, leading to a lack of effective and timely remediation of the known issues. We noted the following required components omitted from the POAM:

- milestone change records and related documentation to justify the changes;
- estimated resources used for the remediation effort and the related justification;
- justification for scheduling estimates and;
- estimated cost with its related justification and the funding source.

Additionally, the POAM includes a field to define specific tasks and milestones; however, this field currently is not being utilized. Therefore, the specific tasks set forth to accomplish this remediation are not documented. Furthermore, the only dates that are defined in the POAM are the start, due, and completion dates for the issue as a whole; thus, the POAM does not define due dates for individual milestones.

Recommendation:

Update the POAM to include the missing information.

FINDING 6: The CPSRMS Security Categorization Document does not adequately justify impact assignments for 10 of the identified information types.

The Categorization Document does not adequately justify impact assignments for 10 of the identified information types, as stipulated by NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*, dated August 2008. For example, OIG found that the “Corrective Action” information type was categorized as “Low” in terms of “Availability.” However, the assignment of this signification was justified in the text of the report using the same logic that was used to raise the “Population Health Management and Consumer Safety” information type from “Low” to “Moderate.” As for the reason for these discrepancies, the agency did not adequately document the justification for the impact assignments for the identified information types. Thus, there is a possibility that the impact assignments are inaccurate, causing an inaccuracy in the solution’s overall impact rating. If the overall impact rating is inaccurate, the amount of effort to protect the solution may not be commensurate with the risk posed by the solution to the agency assets and mission.

In addition, it was noted the Categorization document states: “*Further analysis of data gathered as part of the development of the conceptual architecture and discussions with CPSC is required to establish special factors to raise or lower the impact levels of the security objectives*”; and no additional work has been performed yet.

Please see table below for details surrounding each of the discrepancies.

Information Type Category	Language in Categorization Document	Impact Assigned in the Categorization Document	Appropriate NIST SP 800-60 Impact Assessment based on this language
Corrective Action	Confidentiality: Manufacturers and consumers will provide corrective actions for the various products. The protection of confidentiality	Low	Moderate

	for this information type has a low impact on CPSC, unless the consumer does not want to be identified.		
Corrective Action	Availability: Much like the Population Health Management and Consumer Safety Information Type, users will expect this information to be available 24/7. This is a unique situation where the impact on the CPSC could be severe if the information is not available in a timely manner.	Low	High
Congressional Liaison	Confidentiality: This information may not be made available to the public unless through the public relations information type. If this is CPSC/congressional information, then this information will have a serious impact if confidentiality is compromised. If this was a reporting of public record then this information would be made available to the public and have a low impact.	Low	Moderate
Congressional Liaison	Integrity: The integrity of this information will be important, regardless of whether it is disclosed publicly or remains internal to CPSC. The impact of a compromise of integrity would have a serious impact.	Low	Moderate
Legal Prosecution and Litigation	Confidentiality: The Office of the General Counsel oversees Legal Prosecution and Litigation Type information and may disclose only a portion of the information to the public. The unauthorized disclosure of this information would have a serious impact on the CPSC and require protection.	Low	Moderate
Legal Prosecution and Litigation	Integrity: The integrity of this information, that is the unauthorized modification of legal prosecution and litigation information, would also have a	Low	Moderate

	serious adverse impact on the CPSC and impede the case management system processes.		
General Purpose Data and Statistics	Integrity: The integrity of this information is very important because it is used to perform statistical analysis and is used for decision support analysis. The unauthorized change or modification of this data would have a serious impact on the CPSC.	Low	Moderate
General Purpose Data and Statistics	Availability: Because this information primarily would be used during business hours, the availability of this data would be important and have a serious impact on the CPSC from 6 a.m.–8 p.m.; but if large statistical analyses are run overnight, then the data may be required to be available 24/7.	Low	Moderate
Intellectual Property Protection	Integrity: The integrity of this information must be protected, especially if it is used for litigation purposes. The compromise of integrity for this information type could have a serious impact on the CPSC.	Low	Moderate
Population Health Management and Consumer Safety	Integrity: The compromise of the integrity of this information type could have a serious impact on the CPSC, a manufacturer, and a manufacturer’s public image if the information is not correct. It is critical that this information is accurate.	Low	Moderate

Recommendation:

Perform an assessment to ensure adequate categorization of Information Types and that the logic for categorizing the Information Types as “High,” “Moderate,” or “Low” is consistent with the guidance provided in NIST SP 800-60.

FINDING 7: Insufficient documentation of the analysis disqualifying the non-selected information types in the CPSRMS Security Categorization Document.

The Categorization Document contained justification of the selected information types that were chosen; however, the documentation of the analysis disqualifying the non-selected information types was omitted. Moreover, the Categorization document states: *“At this point in the system lifecycle, it is still unclear whether the identified information types are appropriate and part of the CPSC vision for CPSRMS and its concept of operations”* and no additional work, as yet, has been performed. This occurred, due to a lack of management oversight of the CRI contract and to management not effectively enforcing the stipulations set forth in the CRI Statement of Work. The CPSRMS solution was assigned a “provisional” system impact rating based on the assessment of each of the selected information types documented in the Categorization document. Therefore, any missing or incomplete information in the assessment of these information types, although unlikely, may lead to an inaccurate system impact rating and consequently, may lead to the inaccurate selection of the security controls required by NIST SP 800-53.

Recommendation:

Perform an analysis, as the Categorization document suggests, ensuring that all of the Information Types outlined in the NIST SP 800-60 framework were appropriately included or excluded. Include documentation of this analysis in the Categorization documentation, along with the justification for including and excluding each of the Information Types chosen. Moreover, this analysis should be tied to the Enterprise Architecture. Additionally, CPSRMS’s overall Security Impact assignment should be formalized once this NIST SP 800-60 assessment is completed.

FINDING 8: The CPSRMS SSP does not outline specific Public Access controls in place to mitigate the risks associated with allowing external user’s access to CPSRMS.

The CPSRMS SSP does not outline specific Public Access controls in place to mitigate the risks associated with allowing external user’s access to CPSRMS. OMB A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, dated November 28, 2000 states that “where an agency’s application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.” This is attributable to a lack of management oversight of the CRI contract, and to management not effectively enforcing the stipulations set forth in the CRI Statement of Work. Consequently, without effective controls in place governing Public Access, a public facing information system may provide an entry point for malicious users to the system in an unintended manner (ex. intentionally damage the system or obtain access to sensitive data). Moreover, this lack of control may also allow well-

meaning users to inadvertently damage information system or access sensitive information.

Recommendation:

Define the specific Public Access controls in place/planned, or reference the document defining these controls within the CPRMS SSP.

APPENDIX I: MANGEMENT RESPONSE

PAGE INTENTIONALLY LEFT BANK



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

MEMORANDUM

May 29, 2012

TO: Christopher Dentel, Inspector General

FROM: Patrick D. Weddle
Chief Information Officer
Office of Information and Technology Services

**PATRICK
WEDDLE**

Digitally signed by PATRICK WEDDLE
DN: c=US, o=U.S. Government,
ou=Consumer Product Safety
Commission, cn=PATRICK WEDDLE,
0.9.2342.19200300.100.1.1=610010000
44261
Date: 2012.05.30 06:32:05 -0400

SUBJECT: Management Response to the Office of the Inspector General's Draft Consumer Product Safety Risk Management System Information Security Review Report, May 15, 2012

It is important to note that the IG's report is based on auditing fieldwork that was performed between December 2010 and February 2011. The auditing fieldwork was based on preliminary System and Certification & Accreditation (C&A) documentation that was written between June 2010 and September 2010 with some updates added between September 2010 and December 2010.

Because the preliminary documentation was developed in parallel with the development of the CPSRMS system, that documentation contained incomplete and inaccurate information concerning the CPSRMS architecture, features, security controls implementation and C&A assessments, and, thus the findings in the IG's report are largely out of date.

Due to the state of the preliminary documentation, it was decided to archive that documentation for historical purposes and to totally rewrite the documentation based on an extensive internal assessment of the CPSRMS architecture, business functions, data, system interfaces, and security controls.

The current CPSRMS documentation including System Security Plan (SSP), security controls and C&A assessment was completely rewritten between March and July 2011.

FINDING 1: The draft Risk Management Framework strategy has yet to be formalized or implemented.

Management generally concurs with this finding and the Office of the Executive Director (OEX) will be working with EXIT to establish the CPSC Risk Executive Council and the other associated issues. EXIT staff is soliciting information from other agencies of like size and mission in order to help determine how to best implement the Risk Management function identified in NIST Special Publication - 800-39, Managing Information Security Risk.

FINDING 2: The CPSC has not yet developed an Enterprise Architecture with Information Security considerations.

Management generally concurs with this finding, but, accepts the risk presented by the finding due to the lack of available resources to address it. The risk is deemed low at this point and will be re-evaluated annually.

FINDING 3: Insufficient documentation of the implementation of NIST SP 800-53 security controls in the CPRMS SSP.

Management partially agrees with the finding, but notes that this finding is based on the preliminary documents developed by Communications Resource, Inc. (CRI), which were developed in parallel with the development of the system and therefore contained inaccurate and incomplete information.

After the official launch of CPRMS, the CPRMS and InfoReliance staff performed an extensive internal assessment of the system and did a total rewrite of all documentation including the CPRMS SSP and including updated system architecture, business functions, system interfaces, risk assessment, security categorization, security controls implementation, and security controls assessment.

Furthermore, it was determined that CPRMS consisted of three subsystems: Public Portal, Business Portal, and CPS 360 (internal portal) and that each subsystem required an independent assessment of the security controls. The current version of the CPRMS SSP contains independent assessments of the security controls for each subsystem.

The current version of the CPRMS SSP was updated to be compliant with NIST (SP) 800-53 rev3 and NIST (SP) 800-53A rev1.

Specifically, in reference to recommendation number one of this finding, Management indicates that this type of security control definition would be most appropriately applied during the Requirements Phase of the System Integration Development Lifecycle (SDLC). Because the security controls were not initially included with the CPRMS SDLC, this level of security definition was not possible. However, this level of security control description would be good for future phases of the project if security can be sufficiently integrated within the SDLC.

For recommendation number two, Management notes that the 10 additional controls have been removed from the CPRMS SSP and therefore a cost benefit analysis for those controls is no longer necessary.

For recommendation number three, Management notes that this information is largely improved in the latest version of the CPRMS SSP. Scoping, parameterization, and compensating controls are described where needed in many of the controls.

For recommendation number four, Management notes that the planned controls are documented in section 800-53 of the CPRMS SSP. For new implementations, a security control implementation plan will be developed and included in all planned security controls.

For recommendation number five, Management notes that controls have been updated with the latest internal assessment and Plan of Action and Milestones (POAM).

FINDING 4: The CPSRMS SSP does not reflect the most current information and often contradicts other Security control documents.

Management generally concurs with this finding, and provides the following update:

In reference to recommendation one, all of this work has been performed as part of the internal assessment and rewrite of the CPSRMS SSP performed from March through July 2011. Version 2.4 of the CPSRMS SSP is now the single authoritative document.

In reference to recommendation three, the POAM has been updated in the latest versions of the SSP and POAM tracking database.

FINDING 5: The CPSRMS POAM does not include all elements required by OMB Memoranda 04-25.

Management concurs with this finding and note that the POAM has already been updated according to the IG findings for the latest version of the CPSRMS POAM tracking database (SharePoint site).

FINDING 6: The CPSRMS Security Categorization Document does not adequately justify impact assignments for 10 of the identified information types.

Management concurs with this finding, but, notes that the finding is outdated, as the assessment as recommended has been performed. The latest version of the CPSRMS SSP, version 2.4, published on July 19, 2011 includes Appendix A dedicated to Security Categorization and justification for impact assignments. CPSRMS management and stakeholders selected the six information types.

FINDING 7: Insufficient documentation of the analysis disqualifying the non-selected information types in the CPSRMS Security Categorization Document.

Management partially agrees with this finding; however, management notes that the finding is outdated, as remediation, has been performed. As such, Management notes that the CPSRMS SSP version 2.4 includes Appendix A that describes the security categorization process including the justification of the six information types that were selected by the stakeholders.

Further, Management notes that analysis disqualifying the non-selected information types was not performed. To analyze and document the justification for not selecting the remaining 224 information types would take approximately 112 hours or 14 days at an average of 30 minutes per information

type. It was determined that the time needed to justify the non-selected information types could be used for more critical functions.

FINDING 8: The CPSRMS SSP does not outline specific Public Access controls in place to mitigate the risks associated with allowing external user's access to CPSRMS.

Management concurs with this finding, but, notes that finding is outdated. Management indicated that the CPSRMS SSP version 2.4, published July 19, 2011 describes the NIST (SP) 800-53 security controls implementation to protect public access including Access and Account Management controls (passwords, session controls, account lockout, and eCaptcha) and Cryptographic Controls (SSLv3/TLS).