Office of Inspector General

U.S. Consumer Product Safety Commission

Review of Personal Property Management System and Practices for Calendar Year 2017

May 31, 2019

19-A-06

Vision Statement

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

Statement of Principles

We will:

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

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

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

Be innovative, question existing procedures, and suggest improvements;

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

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

Work together to address government-wide issues.

Office of Inspector General
U. S. Consumer Product Safety Commission

May 31, 2019

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

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Review of Personal Property Management System and Practices for Calendar Year 2017

To ensure that agency policies and procedures regarding personal property management comply with federal requirements, Consumer Product Safety Commission (CPSC) policies, and best practices, the CPSC Office of Inspector General (OIG) retained the services of Kearney & Company (Kearney), an independent public accounting firm. Under a contract monitored by the OIG, Kearney issued a review report regarding the CPSC's personal property management policies and procedures. The contract required that the review be performed in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (CIGIE QSIE).

Among other things, the review found that the CPSC had not implemented sufficient internal controls to ensure that property was properly accounted for and reliable data entered into the CPSC's property management systems. The attached report contains 25 recommendations which, when implemented, will provide management tools to improve internal controls over personal property management and a more effective program. In the next 30 calendar days, in accordance with the Office of Management and Budget's Circular A-50, *Audit Followup* (sic), the CPSC is required to provide me with management's Corrective Action Plan describing the specific actions they anticipate taking to implement each recommendation.

In connection with the contract, we reviewed Kearney's report and related documentation and inquired of its representatives. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. Kearney is responsible for the attached report. However, our review disclosed no instances where Kearney did not comply, in all material respects, with CIGIE's QSIE.

Should you have any questions, please contact me.

THE U.S. CONSUMER PRODUCT SAFETY COMMISSION

Review of Personal Property Management System and Practices for Calendar Year 2017

Report Date: April 7, 2019

Point of Contact:
Kenneth Naugle, Partner
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
knaugle@kearneyco.com
Kearney & Company, P.C.'s TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14.

TABLE OF CONTENTS

Page #

OBJECTIVE 1
BACKGROUND 1
CRITERIA 2
REVIEW RESULTS 2
FINDING 1: INSUFFICIENT RECEIPT AND ACCEPTANCE PROCESS 4
FINDING 2: ESTABLISH POSITION ON CAPITALIZING COMPLIANCE SAMPLES 6
FINDING 3: INSUFFICIENT INVENTORY PROCEDURES 7
FINDING 4: LACK OF DATA RELIABILITY 8
FINDING 5: INADEQUATE PERIODIC CONTROL ASSESSMENT FOR PMS 9
FINDING 6: INADEQUATE POA&M MANAGEMENT 12
FINDING 7: INADEQUATE ACCESS PROVISION MANAGEMENT 14
FINDING 8: INADEQUATE PERIODIC USER ACCESS REVIEW 15
FINDING 9: LACK OF SEPARATION OF DUTIES AT CPSC ORGANIZATIONAL LEVEL 17
FINDING 10: LACK OF SEPARATION OF DUTIES WITHIN THE PMS 18
FINDING 11: INADEQUATE CHANGE MANAGEMENT PROCESS 19
CONCLUSION 20
APPENDIX A – SCOPE AND METHODOLOGY OF THE REVIEW 21
SCOPE 21
METHODOLOGY 21
APPENDIX B – CONSOLIDATED LIST OF RECOMMENDATIONS 22
APPENDIX C – MANAGEMENT'S VIEWS ON CONCLUSIONS AND FINDINGS 24
APPENDIX D – ACRONYMS 25

OBJECTIVE

The objective of this engagement is to ensure that the U.S. Consumer Product Safety Commission's (defined as "CPSC" or "the Commission" in this report) Personal Property Management System (PMS) and property management policies and procedures comply with federal requirements, CPSC policies, and best practices. As requested by the CPSC Office of Inspector General, Kearney & Company, P.C. (defined as "Kearney," "we," and "our" in this report) reviewed the CPSC's personal property transactions recorded in PMS and the Integrated Field System (IFS) between January 1, 2017 and December 31, 2017. Additionally, we reviewed relevant PMS application and information technology (IT) general controls.

BACKGROUND

The Office of Facilities Services (EXFS) is responsible for the oversight of the Commission's property program. The Director of EXFS is responsible for developing policies for and administering control over the CPSC property management program. The Director of EXFS also designates and defines the duties of the Property Management Officer, who holds primary responsibility for personal property management within CPSC.

The individual CPSC offices employ Property Accountable Officers and Property Custodians (PC) who acquire, issue, inventory, and maintain accountability of the Commission's personal property assets. They are also responsible for identifying and, if necessary, disposing of excess property.

In addition, the CPSC collects samples of products either through purchase or donation in pursuit of its mission to protect the public against unreasonable risks of injuries associated with consumer products. The Office of Compliance and Field Services (EXC) is responsible for managing property associated with samples and preventing the untimely or unauthorized destruction of samples by Commission personnel. EXC uses IFS to account for samples and the Sample Tracking System to track the movement of the samples (i.e., testing and storage).

The Office of Financial Management, Planning, and Evaluation holds overall responsibility for the following:

- Preparation and execution of the CPSC's operational budget
- Management of financial systems, reporting, and internal controls
- Direction of the CPSC's strategic planning and performance reporting efforts
- Facilitation of the acquisition process

The Division of Financial Management Service is responsible for assuring the accuracy of the assertions regarding personal property. This includes the authorization, accuracy, existence, obligation, and completeness of the recording of property transactions.

Finally, the Office of Information and Technology Services administers the PMS and is responsible for implementing and overseeing information system controls—both general and application controls—associated with the system.

CRITERIA

Kearney used criteria established by the Federal Government, as listed in ***Exhibit 1***, for testing the CPSC's calendar year 2017 PMS and property management practices.

Exhibit 1: Federal Government Criteria

Description
Federal Property and Administrative Services Act of 1949, as amended
Federal Acquisition Regulation (FAR)
5 Code of Federal Regulations (C.F.R.) 1315.9
41 C.F.R. Chapter 101
41 C.F.R. Chapter 102
41 C.F.R. Chapter 201
48 C.F.R. Chapter 1
Office of Management and Budget (OMB) Circular A-123
OMB Circular A-127
General Services Administration, *Personal Property Utilization and Disposal Guide*
Government Accountability Office's (GAO), *Property Management Systems Requirements*
GAO, *Federal Information System Controls Audit Manual*
GAO, *Standards for Internal Control in the Federal Government* (Green Book)
Statement of Federal Financial Accounting Standards (SFFAS)
National Institute of Standards and Technology (NIST) Special Publications (SP)
CPSC Series 820 policies and procedures
CPSC Series 9010 policies and procedures

REVIEW RESULTS

Kearney noted that CPSC management was able to locate all property assets selected as a part of our sample. However, the CPSC did not implement sufficient internal controls to ensure property was properly accounted for and reliable data was entered into PMS and IFS. Specifically, there was inconsistent recording of property values and appropriately identifying

capitalizable and non-capitalizable assets. The CPSC also did not document a supported position for excluding compliance sample items from its capitalizable assets for financial reporting purposes.

Additionally, the CPSC did not have required application and IT general controls in place and operating to prevent a compromise to the confidentiality, integrity, and availability of the financial data processed in the PMS application.

FINDINGS

Finding 1: Insufficient Receipt and Acceptance Process

Management did not provide evidence to support the receipt and acceptance of goods and services provided to the Commission.

5 C.F.R. 1315.9, *Required Documentation*, identifies required documentation to support the payment of invoices and interest payments. Documentation requirements include specific contract, invoice, and receiving data.

The FAR provides uniform acquisition policies and procedures for use by all executive branch agencies. FAR Part 32.905, *Payment Documentation and Process*, states that "payment will be based on receipt of a proper invoice and satisfactory contract performance." It identifies the content of invoices and specifies that "all invoice payments, with the exception of interim payments on cost-reimbursement contracts for services, must be supported by a receiving report or other government documentation authorizing payment (e.g., government certified voucher)." The receiving report or other government documentation authorizing payment must, at a minimum, include the following:

- Contract number or other authorization for supplies delivered or services performed
- Description of supplies delivered or services performed
- Quantities of supplies received and accepted or services performed, if applicable
- Date supplies delivered or services performed
- Date that the designated government official accepted the supplies or services or approved the progress payment request
- Signature, printed name, title, mailing address, and telephone number of the designated government official responsible for acceptance or approval functions

According to CPSC Order No. 0820.1:

> All receipts and acceptance of personal property shall be documented, whether such personal property is acquired from Government or commercial sources, fabricated in Government shops, donated or recovered. Personal property received and accepted from commercial sources shall be immediately recorded on a receiving report to provide a document of entry to the accounts and records and to substantiate the payment voucher. Receipts of property from other than commercial sources, e.g., donated property, property transferred from another

> agency, fabricated in Government shops or under contract, shall be immediately documented on the appropriate form and entered in the PMS.

Additionally, CPSC Order No. 0820.1 states:

> The PC shall forward a copy of the signed Receiving Report for property…to the Property Management Officer. The PC accepts accountability for the property immediately upon the receipt in his/her organization of a properly executed Receiving Report. The PC shall maintain adequate records so that a complete audit trail can be maintained over all non-expendable personal property.

Based on our review of 52 assets selected as part of a statistical sample consisting of both sample and PMS assets, evidence did not exist to support the receipt and acceptance of 49 assets. Assets consisted of both acquired and donated (i.e., compliance samples) goods obtained through the Commission's procurement processes or through the EXC. EXC obtains samples of products either through purchase or donation for testing purposes in support of its mission to protect the public against risks of injuries associated with consumer products.

Exhibit 2: Property Testing Results

	Compliant	Non-Compliant	Total
IFS	3	14	17
PMS	0	35	35
Total	3	49	52

This condition occurred because the CPSC did not have an effective process in place to receive and document the receipt and acceptance of the deliverables associated with the acquisition or receipt of property donations (e.g., sample items). Instead, the CPSC relied on either receipt forms supplied by vendors or the invoice approval form provided by Department of Transportation Enterprise Services Center, the Commission's vendor processing service provider, which included an acceptance date.

Without adequate evidence of receipt and acceptance, the CPSC does not have assurance that it has received, paid, and accounted for the goods and services for which it obtained.

Kearney recommends that management:

1. Develop and implement a process for receiving and accepting goods and services in accordance with all applicable regulatory requirements. This process should include developing or adjusting an existing government form (e.g., receiving report) that meets

these requirements to standardize the receipt and acceptance of goods and services at the CPSC.

2. Provide training to CPSC personnel on the revised receipt and acceptance process.

Finding 2: Establish Position on Capitalizing Compliance Samples

The CPSC did not include compliance sample items amongst its capitalizable assets for financial reporting purposes. Additionally, the CPSC did not document a supported position for excluding compliance sample items from its capitalizable assets for financial reporting purposes. CPSC Order No. 0820.1 defines personal property as:

> Any property, except real property, records of the Federal Government, cash or instruments that may be used as cash or as payment for anything of value. It includes but is not limited to: supplies; office machines; Information Technology (IT) equipment, including personal computers and peripheral equipment; motor vehicles; furnishings, including carpeting, draperies, and wall decorations; and special use equipment such as laboratory measurement and test equipment, communications, photographic, and duplicating equipment.
>
> Accountable property is property that must be recorded and accounted for in the CPSC Property Management System. Accountable property is generally personal property with an acquisition cost of $500 or more per item or property with an acquisition cost under $500 that has been designated as sensitive property…Certain categories of property with an acquisition cost of $500 or more are excluded from accountable property…It does not include official product samples collected and controlled for compliance and enforcement purposes or other consumer product samples purchased for testing purposes which are tracked in a separate system, the Sample Tracking System.

Further, CPSC Order No. 0820.1 states:

> Capitalized equipment is that accountable non-expendable personal property with an acquisition cost of $5000 or more per item and which is recorded in the General Ledger… Bulk purchases of equipment of $100,000 or more shall be recorded in the General Ledger and depreciated based on class life in accordance with GAO accounting standards.

According to CPSC Order No. 9010.36: "A sample consists of one or more items of evidence collected to provide necessary data and information for CPSC operations."

SFFAS No. 6, *Accounting for Property, Plant, and Equipment*, defines General Property, Plant, and Equipment (PP&E) as:

> [A]ny property, plant, and equipment used in providing goods or services. General PP&E typically has one or more of the following characteristics:
>
> 1. It could be used for alternative purposes (e.g., by other Federal programs, state or local governments, or non-governmental entities) but is used to produce goods or services, or to support the mission of the entity, or
> 2. It is used in business-type activities…

Further, SFFAS No. 6 notes: "All [g]eneral PP&E shall be recorded at cost" to include the "fair value of facilities and equipment donated to the government."

This condition occurred because the CPSC did not consider compliance samples as personal property and, therefore, did not consider these assets for financial reporting purposes. Without fully reporting CPSC property that meets capitalization thresholds, the Commission may not have accurately reported asset balances on its annual financial statements.

Kearney recommends that management:

3. Develop and document a position on whether compliance samples constitute personal property and are subject to capitalization thresholds. This position should be supported with appropriate accounting standards and other applicable criteria.
4. Review this position on a periodic basis to ensure that it remains consistent with current accounting standards.

Finding 3: Insufficient Inventory Procedures

The CPSC did not periodically inventory the compliance sample items acquired or donated to the Commission, even though these assets are stored for at least five years if not destroyed during testing.

According to Green Book, Principle 10.03: "Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system."

This condition occurred because the CPSC did not have procedures in place that required staff to inventory compliance samples.

The CPSC cannot ensure that assets exist and are appropriately accounted for without performing inventories of those assets.

Kearney recommends that management:

5. Develop and implement procedures to periodically inventory compliance sample items.
6. Update the CPSC policies to reflect the new inventory procedures.

Finding 4: Lack of Data Reliability

The CPSC did not have effective controls to ensure the reliability of data entered into the PMS and IFS. For example:

- 1,715 compliance samples, which included all-terrain vehicles, were entered in IFS with an acquisition or market value of $0
- 509 assets, which included highly pilferable items such as iPhones and a digital camera, were entered in the PMS with an acquisition value of $0
- One asset was entered in PMS as non-capitalizable (object class code 312), even though it had a recorded acquisition cost of equal to or greater than $15,000 (approximately $52,000)
- 236 assets were entered in PMS as capitalizable (object class code 311), even though they had a recorded acquisition cost of less than $15,000 (these assets' acquisition costs ranged from $199 to $4,000).

According to Green Book, Principle 11.05:

> Management also evaluates information processing objectives to meet the defined information requirements. Information processing objectives may include the following… Accuracy - Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.

SFFAS No. 6, *Accounting for Property, Plant, and Equipment*, states: "All [g]eneral PP&E shall be recorded at cost" to include the "fair value of facilities and equipment donated to the government."

Prior to July 28, 2014, CPSC Order No. 0820.1 defined the capitalization threshold as:

> "Generally, capitalized equipment is that accountable non-expendable personal property with an acquisition cost of $5,000 or more per item and which is recorded in the General Ledger… Bulk purchases of equipment of $100,000 or more shall be recorded in the General Ledger and depreciated based on class life in accordance with GAO accounting standards."

As of July 28, 2014, CPSC Order No. 0820.01, Amendment No. 1, redefined the capitalization threshold as:

Capitalized equipment is that accountable non-expendable personal property with an acquisition cost of $5000 or more per item and which is recorded in the General Ledger… Bulk purchases of equipment of $100,000 or more shall be recorded in the General Ledger and depreciated based on class life in accordance with GAO accounting standards.
This condition occurred because PMS and IFS did not have sufficient input controls or compensating controls to ensure the reliability of the data entered into the systems or that recorded transactions were consistent with CPSC policies and procedures.

Without reliable data, asset values, including capitalizable assets, may not be recorded and reported accurately for both accountability and financial reporting purposes.

Kearney recommends that management:

7. Develop and implement controls to ensure that the data entered into PMS and IFS is accurate and consistent with CPSC policies and procedures.
8. Develop procedures to review applicable regulations and laws on an annual basis in order to ensure the property management policies and procedures remain accurate and complete.

Finding 5: Inadequate Periodic Control Assessment for PMS

Management has not formally authorized the PMS application to operate in accordance with OMB and NIST guidance. Specifically, management has not

- Properly categorized PMS. As a property management system, PMS is, by definition, a "major information system" requiring an Authorization To Operate
- Performed and documented a risk analysis that justifies not conducting an annual review of the PMS application-specific controls

- Updated the PMS security assessment since 2016, and the 2016 PMS security assessment did not include comprehensive information regarding testing procedures and results of the testing performed
- Performed an annual assessment of the two PMS controls required by the CPSC Information Security Continuous Monitoring (ISCM) Plan.

CPSC's ISCM Plan, Version 4.2, dated July 2017, states:

> Section 4.5.3 Task
>
> An independent assessor will produce security assessment reports for information systems annually—at the completion of ongoing control assessments.
>
> Section 4.6.3. Task
>
> The [Information System Security Officer] ISSO (or delegate) will prepare an Annual Security Status Report of the results of monitoring activities during the period. The purpose of this report is to advise the Authorizing Official on the results of continuous monitoring, what was detected, how risks were mitigated and overall changes to the security and compliance posture.
>
> According to Appendix A, *Security Control Assessment Frequency*, Account Management (control ID AC-2) and Separation of Duties (control ID AC-5) each require an independent assessment annually.

NIST SP 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control RA-3 Risk Assessment
>
> Control: The organization:
>
> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
> b. Documents risk assessment results;
> c. Reviews risk assessment results;
> d. Disseminates risk assessment results; and

e. Updates the risk assessment in accordance with organizational-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, states:

> A Major Application is: an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application...
>
> All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, store, or transmit, or because of their criticality to the agency's mission, require special management oversight. These applications are major applications. A major application is expected to have a [Federal Information Processing Standards] FIPS 199 impact level of moderate or high. OMB Circular A-130 defines a 'major information system' as an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property [emphasis added], or other resources. Major applications are by definition major information systems."

CPSC management miscategorized PMS as a minor application and did so without a formal documented risk analysis justifying the application's categorization or defining the frequency of the PMS security controls review.

By not designing and implementing a process to ensure that security controls are reviewed adequately, the risk of a negative impact to the confidentiality, integrity, and availability of the financial data processed in the PMS application increases.

Kearney recommends that management:

9. Perform and document a formal analysis on the PMS operating environment and system mission to determine the appropriate system categorization for PMS.
10. Upon a justifiable determination of the PMS system categorization, design, implement, and assess the PMS security controls and formally authorize PMS to operate in accordance with CPSC organizational security policies and procedures as well as other applicable government standards.

Finding 6: Inadequate POA&M Management

Although management has a process to track Plan of Action and Milestones (POA&M) for the General Support System (GSS) Local Area Network (LAN) and other major applications, the formal POA&M management practice, as of December 2018, was not adequately designed for tracking PMS application-specific and inherited control weaknesses. Specifically, management has not:

- Defined and documented estimated completion timeline/timeframe by the risk levels defined in the POA&Ms
- Documented the names of the applications that may be affected by each security weakness in the GSS LAN POA&Ms
- Documented POA&Ms and tracked the remediation progress for the two findings identified in the annual GSS LAN Security Assessment Report and one finding resulting from the PMS triennial security review
- Updated the estimated completion dates for 74 of 77 "delayed" status POA&M entries, which were originally scheduled to be completed between 2011 and 2018

CPSC's ISCM Plan, Version 4.2, dated July 2017, states*:*

> Section 4.4.2
>
> The Security Officer then initiates remediation actions on outstanding POA&Ms produced during the ongoing monitoring of security controls by:
>
> a. Consulting with the ISSO to determine the severity or seriousness of the weakness and whether the weakness is significant enough to be worthy of further investigation or remedial action;
> b. Determining the appropriate steps required to correct the identified weaknesses or deficiencies (for those determined to require remedial action);
> c. Developing and documenting (within the POA&M) corrective action plans for the remediation;
> d. Notifying the ISSO (or delegate) when remediation is complete so that assessment can be scheduled and performed (security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions have been taken to eliminate weaknesses or deficiencies or to mitigate the identified risk); and
> e. Updating the POA&M following communication of the assessment results."

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control CA-5 Plan of Action and Milestones
>
> Control: The organization:
>
> a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
> b. Updates existing POA&Ms based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Management did not follow the established POA&M management procedures to track remediation progress for PMS inherited control weaknesses. Regarding the PMS application-specific control weaknesses, management miscategorized PMS as a minor application and did so without a formal documented risk analysis justifying the application's categorization, nor does the Commission track remediation progress for control weaknesses specific to the PMS application.

By not effectively designing and implementing adequate controls to ensure proper POA&M management, the risk of a negative impact to the confidentiality, integrity, and availability of the financial data processed in the PMS application increases.

Kearney recommends that management:

11. Establish and implement POA&M management procedures to ensure that all identified security weaknesses, including PMS application-specific and inherited control weaknesses, are fully documented and tracked.
12. Establish and implement POA&M management procedures to ensure that estimated remediation timeframes are established for security weaknesses and based on the levels of risk and level of effort defined in the POA&Ms.
13. Establish and implement POA&M management procedures to ensure that changes to
14. Estimated completion dates should be documented and reflected in the POA&M tracker.

Finding 7: Inadequate Access Provision Management

Management has not established, documented, and implemented formal user access request procedures for PMS. Specifically, management has not established a process which requires formal management approval prior to granting access to or modifying the access of existing users within PMS.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control AC-1 Access Control Policy and Procedures
>
> Control: The organization:
>
> a. Develops, documents, and disseminates:
> 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
> b. Reviews and updates the current:
> 1. Access control policy; and
> 2. Access control procedures.
>
> "Control AC-3 Access Enforcement
>
> (2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION
>
> The information system enforces dual authorization for organization-defined privileged commands and/or other organization-defined actions.
>
> Supplemental Guidance: Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety. Dual authorization may also be known as two-person control."
>
> Control AC-24 Access Control Decision

> Control: The organization establishes procedures to ensure organization-defined access control decisions are applied to each access request prior to access enforcement.
>
> Supplemental Guidance: Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions.

Management categorized PMS as a minor application and considered it a low-risk system. Therefore, management has not established the application access controls specific to this application.

By not effectively designing and implementing adequate access controls for PMS, the risk of a negative impact to the confidentiality, integrity, and availability of the financial data processed in the PMS application increases.

Kearney recommends that management:

15. Perform and document a formal analysis of PMS's operating environment and system mission to determine the appropriate risk level categorization for PMS.
16. Upon a justifiable determination of PMS's system categorization, design and implement standard procedures for requesting and approving user access to roles and resources in PMS.

Finding 8: Inadequate Periodic User Access Review

Management has not established a periodic review of PMS access for standard and administrator users. Additionally, management has not established procedures describing the detailed process of how administrators validate the roles and responsibilities of the custodian users (e.g., actions taken to come to such conclusion).

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control AC-1 Access Control Policy and Procedures
>
> Control: The organization:
>
> a. Develops, documents, and disseminates:

1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

b. Reviews and updates the current:
   1. Access control policy; and
   2. Access control procedures.

Control AC-6(7) Review of User Privileges

Control: The organization:

(a) Reviews the privileges assigned to validate the need for such privileges; and
(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

While management developed and implemented policies and procedures to perform a periodic review of custodian users' accounts and their associated privileges, the procedures did not include specific guidance on how the control owner should perform the validation of each custodian user's access. Additionally, management has not dedicated the resources required to establish requirements for the periodic review of user access for standard and administrator users.

Failure to appropriately conduct and complete a periodic review of all PMS user accounts increases the risk of inappropriately assigned access privileges. If situations or responsibilities change, users may retain system access beyond the requirements of their daily job functions. Inappropriately assigned or excessive access privileges increase the risk that erroneous or fraudulent transactions could be processed.

Kearney recommends that management:

17. Develop, approve, and implement procedures to ensure that standard users and administrators are included in the periodic review of PMS user access and that the custodian user access is validated appropriately when performing the review.
18. Update the PMS Internal Control Document, or equivalent documentation, to reflect PMS's updated process.
19. Complete and document the periodic review for all PMS users in accordance with PMS's updated procedures.

Finding 9: Lack of Separation of Duties at CPSC Organizational Level

Management has not identified and implemented entity-level separation of duties (SoD) controls to ensure PMS users do not have access rights for other CPSC systems that could lead to a conflict of interest.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control AC-5 Separation of Duties
>
> Control: The organization:
>
> a. Separates;
> b. Documents separation of duties of individuals; and
> c. Defines information system access authorizations to support separation of duties.
>
> Supplemental Guidance: Separation of duties address the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

According to Green Book, Principle 10.12: "Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk."

Management categorized PMS as a minor application. Therefore, management has not performed and documented a formal SoD risk analysis between PMS and other CPSC systems.

Failing to develop and implement an effective process to identify and document SoD conflicts increases the risk that a user may have unauthorized and/or unmonitored conflicting roles on CPSC systems. Users with access privileges that create potential SoD conflicts may perform

functions that impact the integrity of the data within the system and increase the risk of fraudulent activity.

Kearney recommends that management:

20. Perform and document a risk analysis to identify SoD conflicts that may exist between PMS and other CPSC systems.
21. Upon completion of the risk analysis, develop and implement procedures to ensure that CPSC users do not have unmonitored conflicting access across multiple systems.

Finding 10: Lack of Separation of Duties within the PMS

Management has not identified and documented the conflicting roles and responsibilities that may allow PMS users to execute incompatible transactions.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control AC-5 Separation of Duties
>
> Control: The organization:
>
> a. Separates;
> b. Documents separation of duties of individuals; and
> c. Defines information system access authorizations to support separation of duties.
>
> Supplemental Guidance: Separation of duties address the potential for abuse of authorized privileges and helps reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

According to Green Book, Principle 10.12: "Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk."

While management asserts that there are no inherent conflicts of interest inherent within the three PMS roles (i.e., Employee, Administrator, and Custodian), the CPSC has not performed and documented a risk analysis to justify this assertion.

Failing to develop and implement an effective process to identify and document SoD conflicts increases the risk that a user may have unauthorized and/or unmonitored conflicting roles and responsibilities within PMS. Users with access privileges that create SoD conflicts may perform functions that impact the integrity of the data within the system and increase the risk of fraudulent activity.

Kearney recommends that management:

22. Perform and document a risk analysis to identify potential SoD conflicts within PMS.
23. Upon the completion of the risk analysis noted above, management should develop and implement procedures that ensure PMS users do not have sufficient access to allow the unmonitored execution of incompatible transactions.

Finding 11: Inadequate Change Management Process

Management did not follow the standard change management process for PMS changes in accordance with established policies and procedures. Additionally, management did not have the capability to generate a listing of configuration changes made to the PMS application's production environment for the review period.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> Control CM-3 Configuration Change Control
>
> Control: The organization:
>
> a. Determines the types of changes to the information system that are configuration-controlled;
> b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
> c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for organization-defined time period;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for the configuration change control activities through organization-defined configuration change control element (e.g., committee, board) that convenes.

Although management developed a PMS configuration change management process, the Commission did not follow the documented process. Additionally, management stated that PMS does not have the capability to track, log, and generate the listing of changes.

By failing to document changes and maintaining the appropriate supporting documentation for those changes, management may not be fully aware of all the changes made to the PMS application or the extent of the known changes. Further, personnel who do not have this information may not be able to identify configurations that impact the security posture of the information system and the organization.

Kearney recommends that management:

24. Update and implement configuration change management procedures which include requirements to perform and document quality control reviews.
25. Develop and implement procedures to log, track, and maintain a list of changes made to the PMS application.

CONCLUSION

Based on the review results previously noted, Kearney concluded that CPSC management was able to locate all property assets selected as a part of our sample. However, the CPSC did not implement sufficient internal controls to ensure property was properly accounted for and reliable data was entered into PMS and IFS. Specifically, there was inconsistent recording of property values and appropriately identifying capitalizable and non-capitalizable assets. The CPSC also did not document a supported position for excluding compliance sample items from its capitalizable assets for financial reporting purposes.

Additionally, the CPSC did not have required application and IT general controls in place and operating to prevent a compromise to the confidentiality, integrity, and availability of the financial data processed in the PMS application.

APPENDIX A – SCOPE AND METHODOLOGY OF THE REVIEW

Scope

This report contains the results of our review of the CPSC PMS and practices for compliance with applicable laws and regulations and integration of best practices. The scope of this review consisted of a statistical sample of property transactions for CY 2017 extracted from the PMS and IFS. Kearney identified 6,356 assets recorded in PMS and 4,767 assets recorded in IFS. We conducted our review from September 2018 through March 2019 at the CPSC's headquarters in Bethesda, MD; Test and Evaluation Center in Rockville, MD; and storage warehouse in Rockville, MD.

Methodology

Kearney conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*, which requires that we obtain sufficient data to provide a reasonable basis for reaching our conclusions. These standards also require Kearney to ensure that the evidence supporting findings, conclusions, and recommendations is sufficient, competent, and relevant, such that a reasonable person would be able to independently sustain the findings, conclusions, and recommendations. Sufficiency of the data needed and tests of evidence varied based on the review objective, findings, and conclusions. Kearney designed the review to obtain insight into the CPSC's current processes and procedures, as well as to assess compliance with property management requirements and best practices. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our review objective.

APPENDIX B – CONSOLIDATED LIST OF RECOMMENDATIONS

Finding	Recommendation
Finding 1	1. Develop and implement a process for receiving and accepting goods and services in accordance with all applicable regulatory requirements. This process should include developing or adjusting an existing government form (e.g., receiving report) that meets these requirements to standardize the receipt and acceptance of goods and services at the CPSC. 2. Provide training to CPSC personnel on the revised receipt and acceptance process.
Finding 2	3. Develop and document a position on whether compliance samples constitute personal property and are subject to capitalization thresholds. This position should be supported with appropriate accounting standards and other applicable criteria. 4. Review this position on a periodic basis to ensure that it remains consistent with current accounting standards.
Finding 3	5. Develop and implement procedures to periodically inventory compliance sample items. 6. Update the CPSC policies to reflect the new inventory procedures.
Finding 4	7. Develop and implement controls to ensure that the data entered into PMS and IFS is accurate and consistent with CPSC policies and procedures. 8. Develop procedures to review applicable regulations and laws on an annual basis in order to ensure the property management policies and procedures remain accurate and complete.
Finding 5	9. Perform and document a formal analysis on the PMS operating environment and system mission to determine the appropriate system categorization for PMS. 10. Upon a justifiable determination of the PMS system categorization, design, implement, and assess the PMS security controls and formally authorize PMS to operate in accordance with CPSC organizational security policies and procedures as well as other applicable government standards.
Finding 6	11. Establish and implement POA&M management procedures to ensure that all identified security weaknesses, including PMS application-specific and inherited control weaknesses, are fully documented and tracked. 12. Establish and implement POA&M management procedures to ensure that estimated remediation timeframes are established for security weaknesses and based on the levels of risk and level of effort defined in the POA&Ms. 13. Establish and implement POA&M management procedures to ensure that changes to estimated completion dates should be documented and reflected in the POA&M tracker. 14. Estimated completion dates should be documented and reflected in the POA&M tracker.

Finding	Recommendation
Finding 7	15. Perform and document a formal analysis of PMS's operating environment and system mission to determine the appropriate risk level categorization for PMS. 16. Upon a justifiable determination of PMS's system categorization, design and implement standard procedures for requesting and approving user access to roles and resources in PMS.
Finding 8	17. Develop, approve, and implement procedures to ensure that standard users and administrators are included in the periodic review of PMS user access and that the custodian user access is validated appropriately when performing the review. 18. Update the PMS Internal Control Document, or equivalent documentation, to reflect PMS's updated process. 19. Complete and document the periodic review for all PMS users in accordance with PMS's updated procedures.
Finding 9	20. Perform and document a risk analysis to identify SoD conflicts that may exist between PMS and other CPSC systems. 21. Upon completion of the risk analysis, develop and implement procedures to ensure that CPSC users do not have unmonitored conflicting access across multiple systems.
Finding 10	22. Perform and document a risk analysis to identify potential SoD conflicts within PMS. 23. Upon the completion of the risk analysis noted above, management should develop and implement procedures that ensure PMS users do not have sufficient access to allow the unmonitored execution of incompatible transactions.
Finding 11	24. Update and implement configuration change management procedures which include requirements to perform and document quality control reviews. 25. Develop and implement procedures to log, track, and maintain a list of changes made to the PMS application.

APPENDIX C – MANAGEMENT'S VIEWS ON CONCLUSIONS AND FINDINGS

We presented 11 Notices of Findings and Recommendations to CPSC management on March 1, 2019. The CPSC concurred with the findings in responses dated March 14 or 18, 2019. We discussed our observations and conclusions with management at an exit conference on April 23, 2019. Management stated their overall agreement with the results of the review and provided comments that were incorporated into this report, as appropriate.

APPENDIX D – ACRONYMS

Acronym	Definition
C.F.R.	Code of Federal Regulations
Commission	U.S. Consumer Product Safety Commission
CPSC	U.S. Consumer Product Safety Commission
EXC	Office of Compliance and Field Services
EXFS	Office of Facilities Services
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
GAO	U.S. Government Accountability Office
Green Book	GAO Standards for Internal Control in the Federal Government
GSS	General Support System
IFS	Integrated Field System
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
Kearney	Kearney & Company, P.C.
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PC	Property Custodian
PMS	Property Management System
POA&M	Plan of Action and Milestone
PP&E	Property, Plant, and Equipment
Rev.	Revision
SFFAS	Statement of Federal Financial Accounting Standards
SoD	Segregation of Duties
SP	Special Publication

CONTACT US

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

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

On-line complaint form:

Click here for complaint form.

Click here for CPSC OIG Website.

Or **Write:**

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