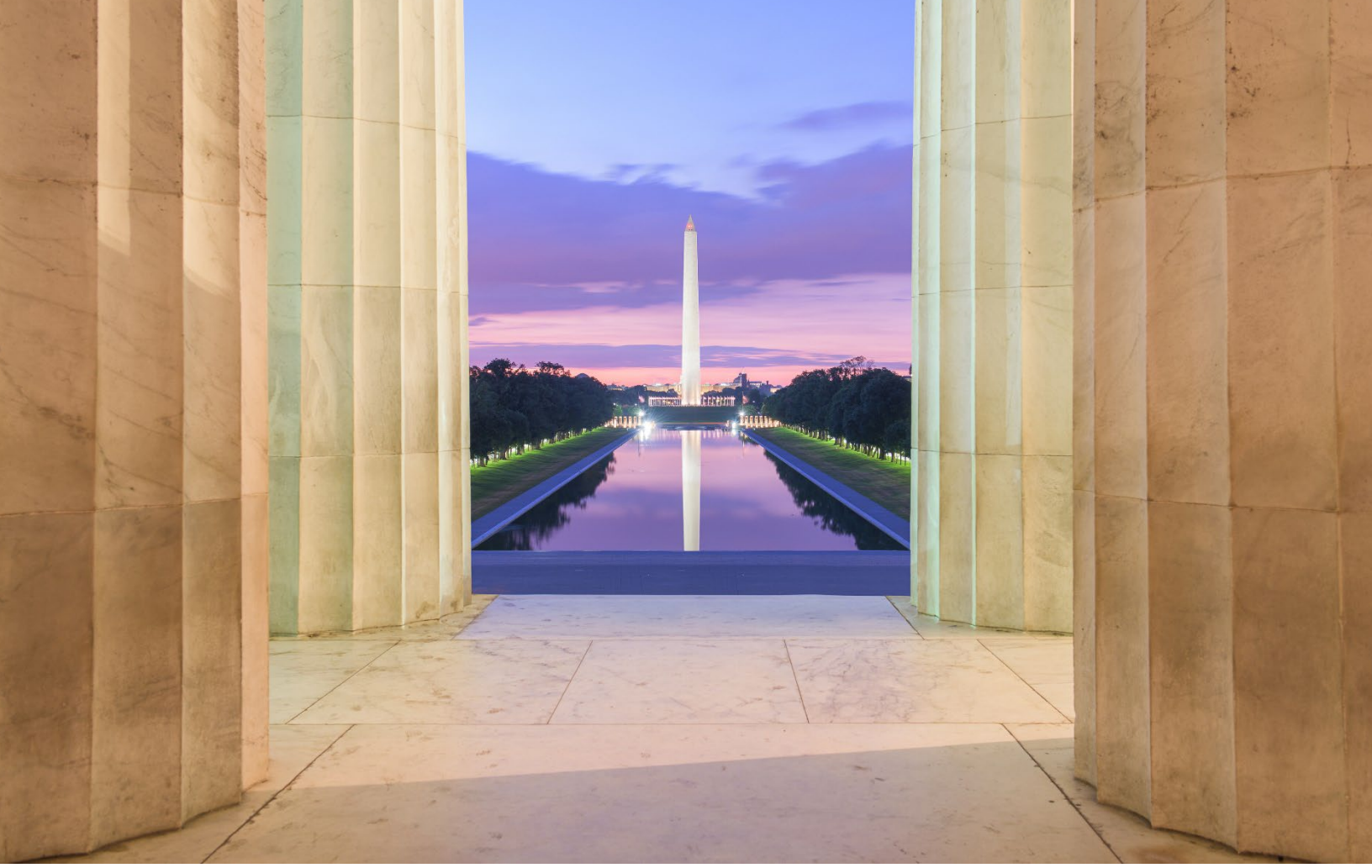
U.S. Consumer Product Safety Commission
OFFICE OF INSPECTOR GENERAL

Top Management and Performance Challenges for Fiscal Year 2024

January 5, 2024

24-O-02



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.

Work together to address government-wide issues.

January 5, 2024

TO: Alexander Hoehn-Saric, Chair
Peter A. Feldman, Commissioner
Richard L. Trumka, Commissioner
Mary T. Boyle, Commissioner

FROM: Christopher W. Dentel, Inspector General Christopher W. Dentel Digitally signed by Christopher W. Dentel Date: 2024.01.05 09:54:48 -05'00'

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2024

In accordance with the Reports Consolidation Act of 2000, I am providing you information on what I consider to be the most serious management and performance challenges facing the U.S. Consumer Product Safety Commission (CPSC) in fiscal year (FY) 2024. Congress left the determination and threshold of what constitutes a most serious management and performance challenge to the discretion of the Inspector General. Serious management and performance challenges are defined as mission critical areas or programs that have the potential to be a significant weakness or vulnerability that would greatly impact agency operations or strategic goals if not addressed by management.

As detailed in the following pages, the CPSC has made marked improvements in several areas related to these management challenges. These improvements include making substantive progress in the past year toward developing a formal system of internal control and revising its directives system. However, despite these improvements, in FY 2024 the most serious management and performance challenges facing the CPSC remain the same as those facing it in FY 2023:

1. Internal Control System
2. Enterprise Risk Management
3. Resource Management
4. Information Technology Security

Moving forward, leadership must do a better job of setting high standards for employees' performance; measuring program effectiveness; ensuring adherence to policies, rules, regulations, and laws; and optimizing the use of limited resources.

Please feel free to contact me if you or your staff have any questions or concerns.

TABLE OF CONTENTS

INTRODUCTION

The fiscal year (FY) 2024 management and performance challenges directly relate to the U.S. Consumer Product Safety Commission's (CPSC) mission to "protect the public against unreasonable risks of injury or death from consumer products" and address the CPSC's Strategic Goal 4: Efficiently and effectively support the CPSC's mission. Unfortunately, as demonstrated by the agency's failure to properly complete its statutorily required annual report on the administration of the Consumer Product Safety Act (CPSA) to the President and Congress for fiscal years 2020, 2021, or 2022; its Real Property Capital Plan in 2022; or to develop a comprehensive corrective action plan to address its information technology (IT) security weaknesses, the CPSC has still not adequately addressed its previously reported top management and performance challenges. The FY 2024 management and performance challenges remain:

1. Internal Control System
2. Enterprise Risk Management
3. Resource Management
4. Information Technology Security

These four topics represent what the Inspector General considers to be the most important and continuing challenges to agency operations. They have remained unchanged for the past several years. In part, this may be due to the fundamental nature of these management challenges. It may also be due to the CPSC having historically not dedicated adequate resources to addressing these challenges. Some are likely to remain challenges from year to year, while others may be removed from the list as progress is made toward resolution. Challenges do not necessarily equate to problems; rather, they should be considered areas most deserving of ongoing focus for CPSC management and staff. As detailed below, agency management has recently made progress in a number of these areas.

The challenges we identified speak to both the foundation of agency operations - internal controls - as well the ability of CPSC to manage risk and respond to changes in the external operating environment and within the agency.

Below is a brief discussion of each management and performance challenge along with examples of management's efforts to address each, as well as links to the Office of Inspector General's (OIG) completed work, and information on planned work related to CPSC's management and performance challenges.

1. INTERNAL CONTROL SYSTEM

Historically, the CPSC has lacked an effective system of internal control. An agency's internal control system is the process used by management to both ensure compliance with laws and regulations and to help the organization achieve its objectives, navigate change, and manage risk. A strong internal control system provides stakeholders with reasonable assurance that operations are effective and efficient, the agency uses reliable information for decision-making, and the agency is compliant with applicable laws and regulations.

Federal standards for internal control are established in the Office of Management and Budget's (OMB) Circular A-123 (A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control.*[1] In 2016, A-123 was updated to reflect the most recent edition of the Government Accountability Office, *Standards for Internal Control in the Federal Government* [2] (Green Book), and the internal control requirements of the Federal Managers Financial Integrity Act (FMFIA).

The Green Book provides managers criteria for designing, implementing, and operating an effective internal control system. The Green Book defines controls and explains how components and principles are integral to an agency's internal control system.

The CPSC has made progress in resolving some internal control findings and recommendations from this office. The OIG acknowledges management's:

- Ongoing efforts at reviewing and revising its directive system.

[1] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf
[2] https://www.gao.gov/products/GAO-14-704G

- Ongoing efforts to revise the management assurance and internal controls program governance, including its internal communication and its processes for consolidating its entity-level checklists responses for the Statement of Assurance (SOA).
- Reported success in meeting its goal to have at least fifty percent of assessable units develop formal internal control programs in accordance with Green Book and A-123.

This management challenge aligns with Strategic Goal 4: Efficiently and effectively support the CPSC's mission.

The CPSC reports its overall compliance with the requirements of A-123 and FMFIA through the Chairman's SOA published annually in the Agency Financial Report. For years, the CPSC has asserted that it had effective internal controls over all programs and complied with applicable laws and regulations. These assertions were made based on the results of signed letters of assurance made by management officials affirming that there were effective internal controls in place in the offices for which they were responsible. As demonstrated in the *Report of Investigation Regarding the 2019 Clearinghouse Data Breach*, numerous management officials made those affirmations despite knowing that the assertions they were making regarding the status of internal controls in their offices were not true.

The CPSC's problems with internal control extend beyond the SOA process. As detailed in our *Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019*, historically, the CPSC has not established and implemented a formal internal controls program over its operations. Additionally, there is a misalignment between how the CPSC identifies programmatic or operational activities, how it measures the performance of these activities, and how it reports these activities.

However, the agency has made substantive progress in the past year toward developing a formal system of internal control. We have not yet had the opportunity to audit management's assertion that, as of the end of FY 2023, it had developed formal internal control programs in accordance with Green Book and A-123 for 7 out of 14 offices that had core processes that support the CPSC's mission. However, it is apparent that agency management has placed both emphasis on and resources

behind this effort that had been lacking in the past. The development of formal internal controls covering approximately half of the agency, combined with the agency having a defined plan to extend internal control coverage over the remainder of the agency, represents a truly foundational step in implementing effective internal controls at the CPSC.

Another area where improvement has been shown involves the agency's system of directives. A fundamental weakness in the CPSC's internal control system historically has been the failure to develop and maintain an up-to-date set of written policies and procedures. This problem was first documented over four years ago in our *Audit of the CPSC's Directives System*. In an effort to address this issue, the Chair directed the Office of General Counsel to take the lead in ensuring that the agency reviews and revises its directives system. Although not yet audited, it appears that this is another area where substantial improvements have been made.

" . . . a recurring challenge at the CPSC, and one which has compounded the difficulty in adequately addressing the CPSC's other internal control deficits, has been the 'tone at the top' of the agency."

This lack of written policies and procedures has resulted in the agency not meeting basic statutory and regulatory requirements. The agency's recent failure to complete mandatory reports to Congress regarding agency operations, as required by the CPSA, and not being aware of the requirement to complete a capital planning report required by OMB, appear to be linked to weaknesses in internal control rather than deliberate acts. In the case of the former, there were no internal controls in place to ensure that these reports were completed. In the case of the latter, there was no process in place to ensure the agency tracked the creation of external requirements.

Historically, a recurring challenge at the CPSC, and one which has compounded the difficulty in adequately addressing the CPSC's other internal control deficits, has been the "tone at the top" of the agency. Senior management officials have repeatedly failed to hold employees accountable for failing to maintain standards. A notable example is the above described "pencil whipping" of letters of assurance. Despite clear evidence that management officials demonstrated a lack of integrity and failed to carry out their duties, agency management elected to not take disciplinary action against the responsible officials. When the CPSC has

taken disciplinary action, it has all too often not been proportional to the offense and has failed to create adequate deterrence against similar future misconduct.

In the past, the internal control deficiencies discovered by the OIG have been found almost exclusively in operational programs. The financial programs, with the notable exception of the Antideficiency Act violations related to the purchase card program reported to the Government Accountability Office in February 2023, generally have had good internal controls. Unfortunately, the ongoing audit of the CPSC's FY 2023 financial statements has found internal control issues in financial programs. These issues include both a lack of commitment to competence and a lack of succession planning. In the context of management challenges, these matters are addressed in greater detail below in the "Resource Management" section. These issues will be fully documented in the FY 2023 financial statement audit report and management letter that are scheduled to be published later in FY 2024.

Recently completed OIG work in this area includes: *Management Alert 23-O-04*, Reports of Investigation Regarding the Clearinghouse Data Breach and Irregularities in the FY 2022 Operating Plan Vote, *Audit of the CPSC's Grants Program*, *Report on the Evaluation of the CPSC's Compliance with the Payment Integrity Information Act of 2019* (PIIA) for FY 2022, *Human Capital Program Assessment*, *Evaluation of the CPSC's Compliance with Tax Withholding Requirements*, and *Evaluation of the CPSC's Federal Information Security Modernization Act (FISMA) Implementation for FY 2023*, *Audit of the CPSC's Implementation of the FMFIA for 2018 and 2019*, and the *Review of National Electronic Injury Surveillance System Data*. Ongoing or upcoming OIG work in this area includes the *Audit of the Consumer Product Safety Commission's Fiscal Year 2023 Financial Statements*, *Resource Utilization Audit*, *Laboratory Accreditation Audit*, and *Import Surveillance Audit*.

2. ENTERPRISE RISK MANAGEMENT

Risk is the effect of uncertainty on agency operations. An effective Enterprise Risk Management (ERM) approach is necessary to identify, prioritize, and mitigate the impact of this uncertainty on the agency's overall strategic goals and objectives. ERM is a proactive approach that

allows agency management to assess threats and opportunities that could affect the achievement of its goals. ERM assists management in striking a thoughtful balance between the potential benefits of innovation and the threats that change can bring. There are multiple frameworks developed by well-regarded independent oversight entities that are designed to facilitate the implementation of an effective ERM program. Most recommend organizations do the following:

- align ERM to mission objectives
- identify risks
- assess risks
- select risk responses
- monitor risks
- communicate and report on risks as conditions change

The 2016 update to A-123 emphasized the importance of having an appropriate risk management process for every federal agency. The guidance includes a requirement that agencies annually develop a risk profile which supports their strategic plan. A-123 requires that the CPSC's risk assessment in the risk profile be discussed each year as part of the agency's strategic review and used to inform planning efforts.

We note that the CPSC has experience using a risk-based methodology for its research and inspection operations. As noted last year, the Office of Financial Management, Planning, and Evaluation has begun work on a risk assessment process for the agency as a whole. In FY 2023, the agency used contractors to perform risk assessments of a number of directorates and larger offices. We encourage the agency to continue these efforts and to consider targeting programs rather than directorates or offices.

This management challenge aligns with Strategic Goal 4: Efficiently and effectively support the CPSC's mission.

Historically, perhaps nowhere was the CPSC's deficits in integrating ERM into its operations clearer than in its decision to remove inspectors from the nation's ports for a prolonged period at the beginning of the pandemic. A mature ERM process would have allowed for a more nuanced approach which would have better balanced the risks to inspectors against the safety of American consumers.

The CPSC's weaknesses in applying the principles of ERM and the resulting negative impact on the CPSC's ability to implement internal controls have been repeatedly noted in past FISMA reviews, including the *Evaluation of the CPSC's FISMA Implementation for FY 2023*, the *Audit of the CPSC's Grants Program*, and the *Report of Investigation Regarding the 2019 Clearinghouse Data Breach*.

As noted above, this is an area where improvements have been reported by agency management. The CPSC reports that they have met their goal of having at least fifty percent of assessable units (7 of 14) conduct risk assessments. The agency also reports that they have a defined plan to extend internal control coverage, including risk assessments, over the remainder of the agency. This represents a truly foundational step in implementing enterprise risk management at the CPSC. Although these assertions have not yet been audited, it is apparent that agency management has placed both emphasis on and resources behind this effort that have been lacking in the past.

The OIG will continue to address ERM as part of its statutory audits and as a component in other planned engagements. An assessment of the CPSC's ERM program as a whole has been included in the OIG's annual audit plan; however, in the past the program was clearly not sufficiently mature to be auditable. This may no longer be the case.

3. RESOURCE MANAGEMENT

This challenge relates to management's stewardship of its resources including human capital, agency funds, and agency assets. This challenge has been exacerbated by uncertainty over agency funding levels and deficiencies in the agency's internal budgeting and performance management processes. For example, there are issues related to the calculations used to determine personnel costs and verify operating costs and performance measures. This complicates efforts to ensure program effectiveness, establish appropriate staff levels, and make determinations regarding the optimal mix of "in house" and contracted work. This complicates the duties of both oversight officials (commissioners, congress, etc.) and agency office heads.

The CPSC must reform its financial reporting and budgetary processes so that these become useful management tools instead of simply paperwork exercises. Such a reform would provide senior management with timely and accurate information, so decision makers understand how financial resources are allocated to agency programs.

The agency needs to assess whether it currently has the right personnel for the mission and is providing the right training, tools, structure, and incentives to achieve operational success. Management must continually assess the agency's needs regarding knowledge, skills, and abilities so that the agency can be effective now and prepare for the challenges of the future. These challenges are complicated by the internal control issues discussed previously and by the transition to a hybrid workplace.

As noted in the *Human Capital Program Assessment*, the CPSC's human capital program does not align with federal regulations and lacks overall accountability. Additionally, the CPSC was not making full use of flexibilities available to it to aid in the recruitment and retention of IT and other professionals; nor was it adequately performing succession planning. These shortcomings, if not corrected, may prevent the CPSC from achieving its mission. Many of the findings and recommendations found in this assessment were over two decades old and were first identified in Office of Personnel Management evaluations in 1998 and 2008; however, these recommendations were never resolved, including a finding that the CPSC had not established a system of accountability to ensure that its human capital program is managed effectively and efficiently.

A recent example of the high cost of failing to retain competence or adequately succession plan occurred during the FY 23 audit of the CPSC's financial statements. Despite being warned repeatedly by this office of the existence of a "key person" risk, created by the agency's over reliance on one individual to both manage financial operations and prepare the financial statements for the agency, the agency did not develop a succession plan to deal with the risk of this individual leaving the agency. When this individual did leave the agency, there was no one competent to perform her duties. This resulted in disruptions to the financial operations of the agency and to its ability to successfully complete its publication of its audited FY 23 financial statements in a timely manner.

During the *Human Capital Program Assessment,* CPSC human capital officials stated that they relied on the Federal Employee Viewpoint Survey (FEVS) results to determine if the human capital program was effectively managed. By that measure, when compared to similarly sized agencies, the CPSC was consistently ranked in the bottom third for employee satisfaction. While employees reported being supportive of the mission, they had concerns about supervision. This measure placed the CPSC at 21st of 29 peer agencies (in the bottom 28 percent). Another FEVS measure, "employee skills to mission match," placed the CPSC at 23rd of 29 peer agencies (in the bottom 20 percent). Finally, with regard to recognition, the extent to which employees feel they are recognized for their performance and innovative contributions to their workplaces, the CPSC ranked 25th of 29 peer agencies (in the bottom 15 percent).

The CPSC needs to implement policies and procedures to secure and safeguard vulnerable assets. Vulnerable assets include physical property and data the agency collects and uses to analyze potential harm to consumers. The CPSC should have adequate policies and procedures in place to safeguard data from unauthorized release and physical assets from misappropriation.

As part of resource management, the agency must incorporate potential improvements to agency operations such as those described in government-wide directives and OIG recommendations to improve the efficiency and effectiveness of the CPSC's mission-related safety operations.

Historically, insufficient resources were allocated to implementing OIG recommendations with which the agency had already concurred. This leads to the continuation of problems that have already been identified and that management has already agreed to address. For example, the agency has not developed a comprehensive corrective action plan to address its IT security weaknesses. In order to properly incentivize management officials, the agency should explicitly take into account the successes and failures of its Senior Executive Service (SES) members and other staff responsible for addressing OIG recommendations in their performance appraisal and performance-based award systems. This would create both a financial incentive and a record of individual senior managers' efforts to implement OIG recommendations. We note the CPSC has indicated that it has included an element in all SES performance

reviews regarding actions taken to address findings made by the OIG. However, it is our understanding that no attempt is made to measure the success or validity of those actions. Instead, credit is given if any action to close the recommendations can be demonstrated.
Implementing existing recommendations designed to improve human capital, financial management, and the protection of assets will allow the CPSC to be more efficient and avoid future costs. Effective resource management will allow the CPSC to be agile while responding to change and support overall agency success.

In FY 2023, the OIG presented 75, and agency management concurred with 67 recommendations and closed 30 recommendations. There are a total of 191 open recommendations as of the end of FY 2023. All of these recommendations were determined to be meritorious by agency management, but some are over nine years old.

This management challenge aligns with Strategic Goal 4: Efficiently and effectively support the CPSC's mission.

Recently completed OIG work related to this challenge includes: *Human Capital Program Assessment*, *Evaluation of the CPSC's FISMA Implementation for FY 2023*, *Audit of the CPSC's Grants Program*, *Report of Investigation Regarding the 2019 Clearinghouse Data Breach*, *Audit of the CPSC's FY 2022 Financial Statements*, and *Independent Risk Assessment of the CPSC's Charge Card Programs*.

The statutory audits and reviews related to financial statements, FISMA, and PIIA address this challenge annually. In addition to the statutorily required audits and reviews, the OIG has ongoing work in the area of space utilization. This audit focuses on both the internal controls governing and the actual space utilization of the agency in light of the transition to hybrid work.

4. INFORMATION TECHNOLOGY SECURITY

In IT, there is competition for the resources required to maintain current systems and the resources required to develop new tools and systems. Additionally, there is competition for resources necessary to meet mission

initiatives and resources required to address the ever-evolving IT security environment. As this office has expressed before, and the agency also noted, the CPSC will not be able to meet current and future demands with its current IT resources. The agency will need to reassess the balance between allocating resources to new systems versus securing and maintaining legacy systems. This challenge is not unique to the CPSC.

The most recent FISMA evaluation found that the CPSC continues to make progress in implementing the FISMA requirements. For example, the CPSC was able to close two recommendations through the continued implementation of its privileged user access management solution. This implementation has allowed the CPSC to enforce Personal Identification Verification card authentication for and adequately restrict access to privileged accounts. The CPSC also made progress on remediating several other FISMA recommendations, specifically, the CPSC:

". . . establishing effective governance and a formalized approach to information security risk management is the critical first step to achieving an effective information security program . . . the CPSC has not taken this critical first step."

- Maintained its ongoing authorization for its major systems and tracked system-level Information Security Continuous Monitoring performance measures and metrics.
- Updated its awareness and training policy.
- Defined its Supply Chain Risk Management policy.
- Developed a Continuity of Operation Plan which includes a business process analysis and business impact assessment for each CPSC-identified Mission Essential Function.
- Encrypted all of its databases, virtual machines, and workstations.
- Implemented an effective mechanism to support the timely reports of its security incidents to the Cybersecurity Infrastructure Security Agency.

However, despite these improvements, we determined that the CPSC still had not implemented an effective information security program in accordance with FISMA requirements. The CPSC has not implemented an effective program because the CPSC has still not taken a formal approach to information security risk management and has not prioritized addressing FISMA requirements and OIG recommendations. The National Institute of Standards and Technology (NIST) provides guidance to federal agencies on establishing effective information security programs. This

guidance postulates that establishing effective governance and a formalized approach to information security risk management is the critical first step to achieving an effective information security program. To date, the CPSC has not taken this first step.

The IT challenges currently facing the CPSC include evolving threats, increasingly sophisticated attacks including state-sponsored attacks, and new compliance requirements. These challenges are further complicated by very high turnover in key positions.

Over the years, this office has identified several security weaknesses in the CPSC's information security internal control policies, procedures, and practices that remain unremedied. These conditions have resulted in the unauthorized disclosure of sensitive information and could result in the unauthorized modification or destruction of data and inaccessibility of services and information required to support the mission of the CPSC.

This management challenge aligns with Strategic Goal 4: Efficiently and effectively support the CPSC's mission.

Recently completed OIG work related to this area includes the: *Evaluation of the CPSC's FISMA Implementation for FY 2023*, *Evaluation of the CPSC's NIST Cybersecurity Framework Implementation*, *Report of Investigation Regarding the 2019 Clearinghouse Data Breach*, *Evaluation of the CPSC's Implementation of the Federal Data Strategy*, *Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems* in 2019, *CPSC Penetration Test 2022*, and *Audit of the CPSC's FY 2022 Financial Statements*.

In addition to the statutorily required audits and reviews, the OIG is conducting work in the area of cloud computing.

CONCLUSION

As discussed above, and in the last several Top Management and Performance Challenges reports, the CPSC faces a number of fundamental management and performance challenges. The most serious of these

deal with the lack of an effective internal control program. If left unaddressed, these have the potential to create significant weaknesses and vulnerabilities that could greatly impact agency operations or strategic goals. However, there is some reason for optimism.

Although not yet complete, the CPSC has made fundamental improvements in its directives system and developed formal internal control systems over a number of its offices. Recently, the CPSC recruited outside personnel to fill several key leadership positions. Hopefully, these new leaders will have greater success addressing the fundamental internal control challenges facing the CPSC than their predecessors.

For more information on this report please contact us at CPSC-OIG@cpsc.gov

To report fraud, waste, or abuse, mismanagement, or wrongdoing at the CPSC go to OIG.CPSC.GOV or call (301) 504-7906

Office of Inspector General, CPSC, 4330 East-West Hwy., Suite 702, Bethesda, MD 20814