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

Top Management and Performance Challenges for Fiscal Year 2025

October 15, 2024

25-O-01

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.

October 15, 2024

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

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL Date: 2024.10.17 16:13:01 -04'00'

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2025

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) 2025. 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 in conducting risk assessments, developing a formal system of internal control, and revising its directives system. However, despite these improvements, in FY 2025 the most serious management and performance challenges facing the CPSC remain similar to those it faced in FY 2024:

1. Enterprise Risk Management
2. Resource Management
3. Information Technology Security

Moving forward, leadership must emphasize 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.

INTRODUCTION

The fiscal year (FY) 2025 management and performance challenges directly relate to the U.S. Consumer Product Safety Commission's (CPSC) mission of "Protecting the public from hazardous consumer products" and address the CPSC's Strategic Goal 4: Efficiently and effectively support the CPSC's mission. The challenges currently facing the CPSC are similar to those reported in previous years. However, I am happy to report that the agency seems to be bringing a new sense of urgency to dealing with many of these issues. Indeed, as noted below, progress has been reported by the agency in a number of areas.

Unfortunately, as demonstrated by the FY 2023 Financial Statement Audit (FSA), which resulted in a finding that the CPSC had a material weakness in its internal control system that played a role in the agency receiving a qualified opinion on its financial statements; lack of compliance with the Payment Integrity Information Act of 2019 (PIIA) for FY 2023; 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, and 2022; its Real Property Capital Plan in 2022; and its ongoing failure 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 2025 management and performance challenges are:

1. Enterprise Risk Management
2. Resource Management
3. Information Technology Security

These three topics represent what the Inspector General considers to be the most important and continuing challenges to agency operations. The issues underlying these challenges are not new. These challenges are not unique to the CPSC. Because the CPSC has historically not dedicated adequate resources to addressing these challenges, despite the agency's current admirable efforts to correct them, they are likely to remain challenges for years to come.

Challenges do not necessarily equate to problems; rather, they should be considered areas most deserving of ongoing focus for CPSC management and staff. The challenges we identify speak to both the foundation of agency operations - internal controls - as well as the ability of the 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 references to the Office of Inspector General's (OIG) completed work, and information on planned work related to the CPSC's management and performance challenges.

1. ENTERPRISE RISK MANAGEMENT

Risk is the effect of uncertainty on agency operations. Traditionally, organizations managed risks by placing responsibilities on unit leaders to manage risks within their areas of responsibility. For example, the Chief Information Officer was responsible for managing risks related to the organization's information technology operations, the Chief Financial Officer was responsible for managing risks related to finance and budget, the General Counsel for legal risks, and so on. This traditional approach to risk management is often referred to as silo risk management whereby each silo leader is responsible for managing risks within their silo.

This traditional approach to risk management has limitations, which could result in significant impending risks going undetected by management. Some risks will "fall between the silos." Also, some risks affect multiple silos in different ways. So, while a silo leader might recognize a potential risk, he or she may not realize the significance of that risk to other aspects of the agency. For example, the director of facilities may adjust leases in a way designed to promote operational efficiencies at the agency without communicating said change with the Chief Financial Officer because they does not realize the potential financial reporting consequences of these changes.

The objective of enterprise risk management (ERM) is to develop a holistic portfolio view of the most significant risks to the achievement of the agency's most important objectives. ERM seeks to create a top-down, enterprise view of all the significant risks that might impact the strategic objectives of the agency. In other words, ERM attempts to take into account all types of risks that might have an impact – both positive and negative – on the accomplishment of the agency's mission.

An effective ERM process should be an important strategic tool for agency leaders. Insights about risks emerging from the ERM process should be an important input to the agency's strategic plan. As management and the commissioners become more knowledgeable about potential risks on the horizon, they can use that intelligence to design strategies to nimbly navigate risks that might emerge. Proactively thinking about risks should provide greater efficiencies by reducing the likelihood that unforeseen risks may emerge that might derail important strategic initiatives for the agency and that kind of proactive thinking about risks should also increase the odds that the agency is better prepared to minimize the impact of a risk event should it occur.

Put another way, an effective ERM approach is necessary to identify, prioritize, and mitigate the impact of 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 should assist 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
- respond to risks
- monitor risks
- communicate and report on risks as conditions change

Office of Management and Budget (OMB) Memorandum A-123 (A-123) is the federal government's standard for federal agencies that defines management's responsibilities for internal control and ERM. 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 assess risks that may impact their strategic plan and take those risks into account in their planning efforts.

A-123 also mandates that agencies comply with Government Accountability Office, *Standards for Internal Control in the Federal Government* (Green Book), and the internal control requirements of the Federal Managers Financial Integrity Act (FMFIA).

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

We note that the CPSC has experience using a risk-based methodology for certain of its operations, for example, for its research and inspection operations. However, it is only relatively recently that the Office of Financial Management, Planning, and Evaluation began developing 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 encouraged the agency to continue these efforts and to consider targeting programs rather than directorates or offices. The agency now reports that by the end of FY 2024, risk assessments had been performed by all assessable units and internal controls have been identified to deal with the risks found by that process.[1]

However, as the agency acknowledges, its efforts in this area to date are still at the pilot program stage. On a foundational level, the CPSC has still not incorporated ERM into its operations. 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

[1] The Audit of the CPSC's Implementation of the FMFIA for 2018 and 2019 found that misalignment existed between how the CPSC identified programmatic or operational activities, how it measured the performance of these activities, and how it reported these activities. Our audit recommended that the CPSC focus on programs that help achieve the agency's mission, e.g. FastTrack, rather than offices, e.g. the Office of Compliance, which are organizational units.

allowed for a more nuanced approach which would have better balanced the risks to inspectors against the safety of American consumers.

Once risks and opportunities are identified through the risk assessment process, they should be addressed through internal controls. Internal controls are the tools used by management to help an entity achieve its objectives. Internal controls can range from providing written delegations of authority, that outline who has authority and responsibility over sensitive tasks; to monitoring and analyzing employee use of computers, to detect and prevent misuse as well as to track employee's use of official time; and to include the creation of written policies and procedures, to guide entity operations.

Historically, the CPSC has lacked an effective system of internal control. Within the federal government, 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 the agency's operations are effective and efficient, use reliable information for decision-making, and are compliant with applicable laws and regulations.

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.
- 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 all assessable units develop formal internal control programs in accordance with Green Book and A-123.

The CPSC's past 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 Federal Information Security Modernization Act (FISMA) reviews, including the *Evaluation of the CPSC's FISMA Implementation for FY 2024*, *Financial Statement Audit for FY 2023*, PIIA for FY 2024, the *Audit of the CPSC's Grants Program*, and the *Report of Investigation Regarding the 2019 Clearinghouse Data Breach*.

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 2024, it had developed formal internal control programs in accordance with Green Book and A-123 for the 14 offices that it had determined 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 the majority of the agency would represent a truly foundational step in implementing effective internal controls at the CPSC.

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

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 reported 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. The Office of General Counsel has developed a process to track, review, and revise agency directives. However, although the development of such a process is a key development and a vital first step in addressing the ongoing issues with outdated written policies and procedures, the agency continues to have challenges in this area. For example, some key Human Capital directives are over a decade old and clearly out of date. Other areas of agency operations suffer from having no written policies or procedure governing their operations.

This lack of written policies and procedures has contributed to the agency not meeting basic statutory and regulatory requirements. The agency's recent failure to comply with PIIA reporting requirements in FY 2024, 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 CPSA reporting requirements, there were no internal controls in place to ensure that these reports were completed. In the case of the capital planning

reporting requirements, 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 "rubber stamping" of letters of assurance. Despite clear evidence that management officials demonstrated a lack of integrity by signing off on statements of assurance that they knew or had reason to know were not accurate, 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 audit of the CPSC's FY 2023 financial statements found a breakdown in internal control over financial programs. These issues included weaknesses in succession and contingency planning, training, and inter-office communication which led, among other issues, to the agency not having appropriate personnel with the required competence in financial management operations and reporting experience in place after the departure of two key personnel from the Office of Financial Management, Planning, and Evaluation. These matters are addressed in greater detail below in the "Resource Management" section. These issues were fully documented in the FY 2023 financial statement audit report and management letter.

Recently completed OIG work in this area includes: *Audit of the Consumer Product Safety Commission's Fiscal Year 2023 Financial Statements*, 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 2023*, *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 2024*, *Audit of the CPSC's Implementation of the FMFIA for 2018 and 2019*, and the *Review of National Electronic Injury Surveillance System Data*. Ongoing OIG work in this area includes the Audit of the Consumer Product Safety Commission's Fiscal Year 2024 Financial Statements and Resource Utilization Audit. Upcoming OIG work in this area includes scheduled evaluations of the CPSC's Budget Process and Senior Executive Service (SES) Performance Management System.

2. 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 makes it difficult 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 management.

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; and allow decision makers to better understand how financial resources are allocated across 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 information technology (IT) and other professionals; nor was it adequately performing succession planning. 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 not 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. As noted, when the report was issued, these shortcomings, if not corrected, could prevent the CPSC from achieving its mission.

A recent example of the high cost of failing to retain competence or adequately succession plan occurred during the FY 2023 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 able to adequately 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 2023 financial statements in a timely manner. It also played a role in the agency receiving a qualified

audit opinion.

The agency enters FY 2025 facing unprecedented turnover in its SES ranks. As a result of a program to incentivize early retirement, fully fifteen percent of its SESs, including a deputy executive director and the Chief Financial Officer, left the agency in the last two weeks of FY 2024. The agency reports that steps have been taken to improve the transfer of information from departing employees. This assertion has not yet been assessed by this office.

The CPSC needs to implement policies and procedures to secure and safeguard vulnerable assets as well as accurately track property as part of its financial operations. 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 both track the value of physical assets and protect them from misappropriation. Issues related to property management were noted in the FY 2023 Financial Statement Audit, where they played a role in the agency receiving a qualified opinion.

As part of resource management, the agency should implement best practices and recommendations, such as those described in government-wide directives from the General Services Administration, Office of Management and Budget, and Office of Personnel Management, as well as GAO and OIG reports, to improve the efficiency and effectiveness of the CPSC's operations.

Audit follow-up is an integral part of good management and is a shared responsibility of agency management officials and auditors. Corrective action taken by management on resolved findings and recommendations is essential to improving the effectiveness and efficiency of government operations. Historically, insufficient resources were allocated to implementing OIG recommendations with which the agency had already concurred. This led to the continuation of problems that had already been identified and that management had already agreed to address.

The agency appears to be placing much greater emphasis on this area of late with senior management officials becoming directly involved in the audit follow-up process. This has clearly led to a greater effort on the part of management officials to attempt to implement recommendations. For example, the agency took steps to address recommendations relating to human capital and internal control issues which, despite having been concurred with, had gone years without being directly addressed.

Despite the positive developments noted above, there remains room for improvement. For example, the agency has not developed a comprehensive corrective action plan to address its IT security weaknesses, see "Information Technology Security" below for greater detail. In order to properly incentivize management officials, the agency should explicitly take into account the successes and failures of its 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 does include an SES performance metric

regarding actions taken to address findings made by the OIG. However, the metric does not appear to measure the success or validity of those actions only whether the attempts were timely.

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.

Recently completed OIG work in this area includes*: Audit of the Consumer Product Safety Commission's Fiscal Year 2023 Financial Statements*, *Audit of the CPSC's Grants Program*, *Human Capital Program Assessment*, *Evaluation of the CPSC's FISMA Implementation for FY 2024*, and *Audit of the CPSC's Position Designation and Suitability Program*. Ongoing OIG work in this area includes the Audit of the Consumer Product Safety Commission's Fiscal Year 2024 Financial Statements and the Resource Utilization Audit. Upcoming OIG work in this area includes scheduled evaluations of the CPSC's Budget Process and SES Performance Management System and the Evaluation of the CPSC's FISMA Implementation for FY 2025.

3. 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 risks and benefits of allocating resources to new systems versus securing and maintaining legacy systems. This challenge is not unique to the CPSC.

During the FY 2024 FISMA evaluation, the CPSC's compliance with the annual FISMA reporting metrics set forth by the Department of Homeland Security and the Office of Management and Budget was assessed. It was found that improvements have occurred in some areas. The CPSC was able to close eight recommendations. Specifically, since the FY 2023 FISMA evaluation, the CPSC had:

- established and implemented policies and procedures to manage software licenses using automated monitoring and expiration notifications
- established and implemented a policy and procedure to ensure that only authorized hardware and software execute on the agency's network
- developed, implemented, and disseminated a current configuration management policy which is in accordance with the most recent National Institute of Standards and Technology guidance (NIST)
- identified and documented the characteristics of items that are to be placed under

Configuration Management control
- developed and implemented a Configuration Management plan to ensure it includes all requisite information
- identified and documented potentially incompatible duties permitted by privileged accounts

However, despite these improvements, it was 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 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 critical 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 the high rate of turnover in key positions over the past few years.

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.

Recently completed OIG work in this area includes: *Audit of the Consumer Product Safety Commission's Fiscal Year 2023 Financial Statements*, *Report of Investigation Regarding the Clearinghouse Data Breach*, *Evaluation of the CPSC's FISMA Implementation for FY 2024*, *Evaluation of the CPSC's Management of Cloud Computing, Shared Services, & Third-Party Systems*, *CPSC Penetration Test 2022*; and *Evaluation of the CPSC's NIST Cybersecurity Framework Implementation*. Ongoing OIG work in this area includes the Audit of the Consumer Product Safety Commission's Fiscal Year 2024 Financial Statements. Upcoming OIG work in this area includes the scheduled Evaluation of the CPSC's FISMA Implementation for FY 2025.

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