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

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FOR FISCAL YEAR 2022

October 21, 2021

22-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 21, 2021

TO: Alexander Hoehn-Saric, Chairman
Robert S. Adler, Commissioner
Dana Baiocco, Commissioner
Peter A. Feldman, Commissioner

FROM: Christopher W. Dentel, Inspector General CHRISTOPHER DENTEL Digitally signed by CHRISTOPHER DENTEL Date: 2021.10.20 12:07:38 -04'00'

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2022

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) 2022. 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.

We anticipate that there will be new senior leadership in several key positions at the CPSC in FY 2022. As detailed in the following pages, the challenges facing these new leaders will be magnified by the ongoing pandemic, changes caused by the anticipated return of the workforce to the office, an anticipated increase in agency resources, and a series of missteps made by previous leadership.

Moving forward, leadership must do a better job of setting high standards for employees' conduct and performance, measuring program performance appropriately, and holding employees accountable.

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

TABLE OF CONTENTS

INTRODUCTION....2
INTERNAL CONTROL SYSTEM....3
ENTERPRISE RISK MANAGEMENT....5
RESOURCE MANAGEMENT....7
INFORMATION TECHNOLOGY SECURITY....9

INTRODUCTION

The fiscal year (FY) 2022 management and performance challenges directly relate to the U.S. Consumer Product Safety Commission's (CPSC) mission of "Keeping Consumers Safe" and address both the strategic goals and cross-cutting priorities which support the CPSC's mission. Although the ongoing pandemic has created challenges for the agency, these challenges are addressed across the management and performance challenges listed below rather than as a separate standalone challenge. Our work over the past year has evidenced that, although improvements have occurred in some areas, there has been an overall regression in the CPSC's efforts to establish an appropriate "tone at the top", to implement an effective internal control system over agency operations, and to implement past OIG recommendations. The FY 2022 management and performance challenges are:

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. 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 of continuing focus for the CPSC management and staff.

Change brings both challenges and opportunities. The challenges we identified 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 within the agency and in the external operating environment.

Below is a brief discussion of each management and performance challenge. This includes examples of management's efforts to address each challenge, as well as links to the OIG's completed work, and information on planned work related to the CPSC's management and performance challenges.

1. INTERNAL CONTROL SYSTEM

An agency's internal control system is a process used by management 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 Office of Management and Budget's (OMB) Circular A-123 (A-123), *Management's Responsibility for Enterprise Risk Management and Internal Control*. In 2016, A-123 was updated to reflect the most recent edition of Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (Green Book), and the internal control requirements of the Federal Manager's Financial Integrity Act (FMFIA).

" . . . the CPSC has not established and implemented a formal internal controls program over its operations."

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 work:

- revising the procedures governing the statement of assurance process to better align with their performance-based budget
- providing training to senior managers on their responsibilities regarding the statement of assurance process
- working toward closing internal control recommendations related to the telework, grants, and NEISS programs
- attempting to increase the resources dedicated to improving agency internal controls by requesting 3 new employees for this purpose in the FY 2023 budget justification

The CPSC reports its overall compliance with the requirements of A-123 and FMFIA through the Chairman's statement of assurance 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 Clearinghouse Data Breach Investigation, 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 the Federal Managers' Financial Integrity Act, 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.

Similarly, the recent Review of the CPSC's NEISS Program determined that the NEISS program did not have an adequate data governance program in place to ensure data quality. Additionally, the CPSC could not provide documentation to establish that a legal opinion was obtained before the CPSC expanded the NEISS program to include data on injuries outside of the CPSC's jurisdiction. Finally, the CPSC could not provide sufficient documentation to support estimated costs charged to other federal agencies as required by the Economy Act when using Interagency Agreements.

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 agency management has 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.

A fundamental weakness in the CPSC's internal control system is the agency's failure to develop and maintain an up-to-date set of written policies and procedures. This problem, first documented over two years ago in our Audit of the CPSC's Directives System, has never been adequately addressed. Although some offices have begun utilizing the new directives process developed as a result of that audit, other offices have not and entirely too many areas of agency operation are either governed by out-of-date directives or lack formal directives.

As noted above, the OIG has found serious issues related to internal control deficiencies in a number of areas; however, these problems are almost exclusively limited to operational programs.

This management challenge aligns with the CPSC's cross-cutting priority, Operational Excellence, which supports all four agency strategic goals by developing an effective administrative management foundation to support agency operations.

Recently completed OIG work related to this CPSC cross-cutting priority includes: Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Audit of the CPSC's Grants Program, Evaluation of CPSC's FISMA Implementation for FY 2020, Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019, Review of the CPSC's Compliance with the Payment Integrity Information Act for Fiscal Year 2020, and the Audit of the CPSC's NEISS Program.

Ongoing or upcoming OIG work in this area includes: evaluation of the CPSC's FISMA implementation for FY 2021 and audit of the CPSC's compliance with the Digital Accountability and Transparency Act.

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 OMB 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. OMB 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. Although the Office of Financial Management, Planning, and Evaluation has begun work on a risk assessment process for the agency, very little progress has occurred in this area due to a lack of resources and support by senior management. We encourage the agency to properly resource and expand these risk management efforts to include its support operations and to allocate resources to the areas of greatest opportunities for improvement in agency programs.

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.

"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."

This management challenge aligns with the CPSC's cross-cutting priority, Data Collection and Analysis, which supports all four agency strategic goals by focusing on the collection and use of high-quality data to shape program strategies and prioritize program activities.

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 Federal Information Security Modernization Act (FISMA) reviews, including the Evaluation of CPSC's FISMA Implementation for FY 2020, the most recently completed FISMA review, the Audit of the CPSC's Grants Program, and the Report of Investigation Regarding the 2019 Clearinghouse Data Breach.

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 on the OIG's annual audit plan; however, it is unclear if the agency's program is sufficiently mature to be auditable.

3. RESOURCE MANAGEMENT

This challenge relates to management's stewardship of its resources including human capital, agency funds, and agency assets. This challenge is exacerbated by both the pandemic and the anticipated substantial increase in agency funding projected to occur over the next few years.

The agency needs to assess whether it currently has the right personnel for the job 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 have been highlighted by the adoption of full-time telework due to the ongoing pandemic.

The CPSC must develop and operate financial management systems to provide senior management with timely and accurate information so decision makers understand how financial resources are allocated to agency projects. Agency spending should accurately reflect the policy priorities of the Commission.

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.

The agency would improve the efficiency and effectiveness of the CPSC's mission-related safety operations by incorporating improvements described in government-wide directives and OIG recommendations.

All too often, insufficient resources are allocated to implementing OIG recommendations with which the agency has already concurred. This

leads to the continuation of problems that have already been identified and that management has already agreed to address.

In FY 2021, the OIG presented and agency management concurred with 99 recommendations. During the same time period, agency management resolved only 20 recommendations. There are a total of 215 open recommendations. A number of these recommendations, all of which were determined to be meritorious by agency management, are over eight years old.

As previously discussed with senior agency management, the agency should explicitly take into account the resolution of OIG recommendations in the performance appraisal and performance-based awards of its Senior Executive Service (SES) members and other staff responsible for addressing OIG recommendations. 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 regarding actions taken to address findings made by the OIG in all SES performance reviews. 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.

"There are a total of 215 open recommendations. A number of these recommendations, all of which were determined to be meritorious by agency management, are over eight years old."

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, to mitigate risks to its resources, and to support overall agency success.

The agency has made strides in updating its telework policies and procedures. The telework program has proven to be essential in the agency's transition to full-time telework and will continue to play a key role in its adoption of a hybrid work environment.

This management challenge aligns with the CPSC's Strategic Goal 1: Cultivate the most effective consumer product safety workforce. It also supports all four agency strategic goals by addressing the cross-cutting priority of Operational Excellence, focused on enhancing resource management.

Recently completed OIG work related to this CPSC goal and cross-cutting priority include: Audit of the CPSC's Grants Program, Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Audit of the CPSC's Financial Statements for 2020, The Office of Inspector General's Survey on the Transition to Mandatory Fulltime Telework, Independent Risk Assessment of the CPSC's Charge Card Programs, and the Results of the OIG Survey on Returning to the Workplace.

The statutory audits and reviews related to financial statements, FISMA, and the Payment Integrity Information Act address this challenge annually. In addition to the statutorily required audits and reviews, the OIG has ongoing work in the area of Human Resource Management Practices.

4. INFORMATION TECHNOLOGY SECURITY

In information technology (IT), there is competition for resources required to maintain current systems and the resources needed 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 FY 2020 FISMA evaluation found that the CPSC continues to make progress in implementing the FISMA requirements. For example, the CPSC had:

- continued development of a formal Enterprise Architecture
- made progress on completing Plans of Actions & Milestones
- continued the implementation of technology to support privileged user account management
- hired an additional person to support the privacy program

- continued the implementation of Information Security Continuous Monitoring (ISCM) program system level requirements
- further enhanced network defenses by baselining network activity through the use of network profiling techniques
- performed some business impact analysis tasks to enhance contingency planning

Additionally, in FY 2020 and FY 2021, the CPSC conducted training regarding the importance of protecting both Personally Identifiable Information and section 6(b) information.[1]

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 not taken a formal approach to information security risk management and has not prioritized its limited resources to addressing FISMA requirements and the related recommendations. The National Institute of Standards and Technology issues guidance to federal agencies to establish 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.

". . . 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."

The IT challenges currently facing the CPSC include evolving threats, increasingly sophisticated attacks, new compliance requirements, and state sponsored attacks on government IT assets, and also the challenges presented by the remote work environment adopted to deal with the pandemic. These challenges will continue as the CPSC transitions to a hybrid work environment.

Over the years, this office has identified several security weaknesses in the CPSC's information security internal control policies, procedures, and practices that remain unremediated. These conditions have resulted in the unauthorized disclosure of sensitive information and could result in

[1] Section 6(b) refers to Section 6(b) of the Consumer Product Safety Act (CPSA) which prohibits the Commission from disclosing information about a consumer product that identifies a manufacturer or private labeler unless the Commission has taken "reasonable steps" to assure 1) that the information is accurate, 2) that disclosure of the information is fair in the circumstances, and 3) that disclosure of the information is reasonably related to effectuating the purposes of the CPSA and of the other laws administered by the Commission.

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 the CPSC's cross-cutting priority, Information Technology, which supports all four agency strategic goals by addressing the role of information technology as an integral tool to meet agency objectives.

Recently completed OIG work related to this CPSC cross-cutting priority includes the: Evaluation of CPSC's FISMA Implementation for FY 2020, Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems, and Audit of the CPSC's Financial Statements for FY 2019 and 2020.

In addition to the statutorily required audits and reviews, the OIG is either in the process of assessing or has planned work related to this CPSC cross-cutting priority in the areas of records management, Privacy Act implementation, enterprise architecture, and Evaluation of the CPSC's Implementation of the Cybersecurity Framework.

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