



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



**Top Management and Performance Challenges
for Fiscal Year 2023**

October 28, 2022

23-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 28, 2022

TO: Alexander D. Hoehn-Saric, Chairman
Peter A. Feldman, Commissioner
Richard Trumka Jr., Commissioner
Mary T. Boyle, Commissioner

FROM: Christopher W. Dentel, Inspector General

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2023

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) 2023. 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.

FY 2022 brought the CPSC new senior leadership in several key positions; a trend that appears likely to continue in FY 2023. As detailed in the following pages, the challenges facing these new leaders will be magnified by the ongoing pandemic, ongoing return of the workforce to the office, uncertainty regarding the agency's budget, 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 effectiveness, and optimizing the use of limited resources.

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.....	6
Resource Management.....	7
Information Technology Security.....	10
Conclusion	13



INTRODUCTION

The fiscal year (FY) 2023 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. The end of fulltime telework and the implementation of a "hybrid work environment" have compounded existing challenges related to the internal controls over the management and measurement of the performance of the agency. These issues are addressed across the management challenges listed below rather than as a standalone challenge. Based on our work in FY 2022, it appears that the CPSC has made some progress in its efforts to establish an appropriate "tone at the top," to implement an effective internal control system over agency operations, and to resolve past OIG recommendations. The FY 2023 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. They have remained unchanged for the past several years. In part, this may be due to the fundamental nature of management challenges. It may also be due to the CPSC's failure to adequately address 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 continuing focus for 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 the ability of the CPSC to manage risk and respond to changes inside and outside of its operating environment.

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 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 controls 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*.¹ In 2016, A-123 was updated to reflect the most recent edition of 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 identified by this office. The OIG acknowledges management's work:

- initiating a review and revision of its directive system
- providing training to senior managers on their responsibilities regarding the statement of assurance process
- attempting to increase the resources dedicated to improving agency internal control by requesting three new employees for this purpose in the FY 2023 budget justification

This management challenge aligns with 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.

¹ https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf

² <https://www.gao.gov/greenbook>

The CPSC reports its overall compliance with the requirements of OMB A-123 and FMFIA through the Chairman’s Statement of Assurance (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 statement 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 controls extend beyond the SOA process. As detailed in our Audit of the CPSC’s Implementation of FMFIA for FYs 2018 and 2019, the CPSC has not established and implemented a formal internal control 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.

“ . . . the CPSC has not established and implemented a formal internal control program over its operations.”

Similarly, the Review of National Electronic Injury Surveillance System Data (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 fundamental weakness in the CPSC’s internal control system has been the agency’s failure to develop and maintain an up-to-date set of written policies and procedures. This problem, first documented over three years ago in our Audit of the CPSC’s Directives System, has to date not been adequately addressed. However, on September 21, 2022, the General Counsel announced that, at the initiative of the Chair, the CPSC was embarking on a new effort to review and revise its directives system. This



represents a key potential change in the management of the agency. However, in the past, numerous offices have resisted agency efforts to require them to update their directives and, to date, entirely too many areas of agency operation are either governed by out-of-date directives or lack formal written guidance entirely.

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 statements of assurance. Despite clear evidence that management officials demonstrated a lack of integrity and failed to carry out their duties, agency management elected not to 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 deterrence against similar future misconduct.

The CPSC's failure to take appropriate disciplinary action against the employee responsible for its FY 2014 Antideficiency Act (ADA) violation may well have contributed to its subsequent FY 2019 ADA violation. The perpetrator of the FY 2014 ADA violation admitted to working during the government shutdown despite receiving a written order from the Executive Director ordering him not to do so. Despite his admission to a willful violation of the Antideficiency Act and insubordination, he received no substantive disciplinary action.³ The agency's failure to both take appropriate disciplinary action and to publicize the violation and its consequences within the agency appear to have played a role in the FY 2019 ADA violation, which again, involved a CPSC employee working during the government shutdown contrary to written order and without legal authority. There is new senior leadership at the CPSC and we are hopeful that there will be improvements in these areas.

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. The financial programs, with the notable exception of recent issues related to the purchase card program, generally have good internal controls.

Recently completed OIG work related to this CPSC cross-cutting priority includes the: Report of Investigation Regarding the 2019 Clearinghouse

³ The discipline in question consisted of a "reprimand."

Data Breach, Audit of the CPSC's Grants Program, Report on the Evaluation of the CPSC's Compliance with PIIA for FY 2021, Evaluation of the CPSC's Federal Information Security Modernization Act (FISMA) Implementation for FY 2022, Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019, and Review of National Electronic Injury Surveillance System Data Program. Ongoing or upcoming OIG work in this area includes the FY 2022 Financial Statement Audit, the Import Surveillance Audit, and the Evaluation of the CPSC's FISMA Implementation for FY 2023.

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. 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. However, due to a

lack of resources and support by senior management, very little progress has occurred in this area. 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.

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.

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 2022, 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 has been exacerbated by uncertainty over agency funding levels. The agency planned for but did not receive a substantial increase in agency funding last year. Its current planning is based on what appears to be an overly optimistic expectation of future funding. Further, the agency's internal budgeting and performance management processes are less than

fully transparent. For example, there are issues related to the calculations used to verify operating costs and performance measures. This complicates efforts to establish program effectiveness, appropriate staff levels, and make determinations regarding the optimal mix of work performed “in house” and work that is contracted out. This complicates the duties of both oversight officials (commissioners, congress, etc.) and agency office heads.

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 addressed previously and have been heightened by the transition from fulltime telework during the pandemic to a hybrid workplace.

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.

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 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. This is an area in which the agency has recently shown great improvement. In FY 2022, 67 recommendations were closed, as opposed to 20 in FY 2021. This improvement appears to have been largely driven by the new Chair’s emphasis on closing recommendations and new agency reporting

requirements contained in the FY 2022 Operating Plan.

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 2022, the OIG presented, and agency management concurred with, 55 recommendations. There are a total of 151 open recommendations. A number of these recommendations, all of which were determined to be meritorious by agency management, are over nine years old.

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 includes the: Audit of the CPSC's Grants Program, Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Audit of the Consumer Product Safety Commission's Fiscal Year 2021 Financial Statements, 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's Survey on Returning to the Workplace.



The statutory audits and reviews related to financial statements, FISMA, and Payment Improvement Integrity Act address this challenge annually. In addition to the statutorily required audits and reviews, the OIG has ongoing work in the area of Human Capital Management Practices. This evaluation focuses on human capital management. One of the reasons we chose to initiate the human capital evaluation was due to complaints we received from senior management officials that the CPSC was not making full use of flexibilities available to aid in the recruitment and retention of hard-to-fill positions such as in information technology (IT) and other specialized fields.

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.

A challenge that is unique to the CPSC is the degree of turnover that has taken place amongst senior IT officials in FY 2022. There has been turnover in three of the four most key IT security positions in the agency, including that of the Chief Information Officer. As of the writing of this report, the CPSC has not found permanent replacements for any of these positions.

The Evaluation of the CPSC's FISMA Implementation for FY 2022 found that the CPSC continues to make progress in implementing the FISMA requirements. For example, the CPSC had:

- begun implementing a corrective action plan for the Federal Managers' Financial Integrity Act audit report that will integrate ERM as part of the CPSC's development and review of internal control over IT and other programs
- established a Change Control Board Charter which formalized the roles and responsibilities of the Change Control Board members

- migrated to a new Security Event and Incident Management tool to improve log aggregation and alerting, as well as to improve integration with the CPSC's other incident response tools
- utilized profiling techniques to baseline expected activities on its networks and systems, so that it can more effectively detect security incidents and meet performance metrics

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 (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.

“... 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 the agency's move to a remote work environment. This environment was originally adopted to deal with the pandemic and continues 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 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 the CPSC's FISMA Implementation for FY 2022, Evaluation of the CPSC's NIST Cybersecurity Framework Implementation, Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Report on the Penetration and Vulnerability Assessment of the CPSC's Information Technology Systems, and Audit of the Consumer Product Safety Commission's Fiscal Year 2021 Financial Statements.

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 enterprise architecture, and penetration testing.

CONCLUSION

As discussed above, the CPSC faces a number of serious management and performance challenges. 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 reason for optimism.

FY 2022 brought the CPSC new senior leadership in several key positions; and there seems to be greater comity between commissioners than in the recent past. Indeed, current senior agency management, both career and political, appear more willing to address the challenges facing the CPSC, by implementing OIG recommendations and in other ways, than their predecessors.

However, much work remains to be done. Moving forward, leadership must do a better job of setting high standards for employees' conduct and performance, measuring program effectiveness, and optimizing the use of limited resources.



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