Office of Inspector General

U.S. Consumer Product Safety Commission

Top Management and Performance Challenges for Fiscal Year 2021

October 9, 2020

Report 21-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.

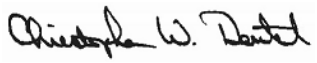
Build relationships with program managers based on a shared commitment to improving program operations and effectiveness.

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

Work together to address government-wide issues.

October 9, 2020

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

FROM: Christopher W. Dentel, Inspector General 

SUBJECT: Top Management and Performance Challenges for Fiscal Year 2021

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 in fiscal year 2021. 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 seriously impact agency operations or strategic goals if not addressed by management.

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

Table of Contents

Introduction

The fiscal year (FY) 2021 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. Our work in these areas indicates that while improvements are needed, the CPSC is making progress toward implementing Office of Inspector General (OIG) recommendations and improving the efficiency and effectiveness of its programs. The FY 2021 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 CPSC management and staff.

These challenges focus on change and how uncertainty impacts CPSC operations. 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 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 OIG's completed work and information on planned work related to 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 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*.[1] 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*[2] (Green Book), and the internal control requirements of the Federal Manager's 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 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. As of FY 2019, the Chairman asserted that the CPSC had effective internal controls over all programs and complied with applicable laws and regulations.

The CPSC has made progress in resolving internal control findings from this office, and has implemented a number of significant recommendations from earlier audits. The OIG acknowledges management's work:

- Strengthening internal controls over the amortization and depreciation process regarding plant, property, and equipment
- Implemented internal controls regarding lab accreditation
- Continued work toward closing internal control recommendations related to the telework program

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.

The OIG has found serious issues related to internal control deficiencies in a number of programs. Most notably, problems have been found that call into question the

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

accuracy of some of the statements of assurance relied upon by the agency in making its annual overall statement of assurance. 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, Review of the CPSC's Compliance with IPERA for FY 2019 , and Evaluation of CPSC's Federal Information Security Modernization Act (FISMA) Implementation for FY 2019.

The OIG is currently reviewing the CPSC's implementation of the FMFIA and the internal controls over its National Electronic Injury Surveillance System (NEISS). The OIG also plans to conduct other audits or reviews of the agency's internal control implementation in FY 2021.

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 response
- 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 coordinates with their strategic plan. The OMB Circular 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. Further, the Office of Financial Management, Planning, and Evaluation has begun work on a risk assessment process for the agency. We encourage the agency to expand these risk management efforts to its support operations and 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.

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 2019, the most recent FISMA review currently in process, 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 reviews, as well 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.

The agency needs to assess whether it has the right personnel for the job on board and are 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 fulltime 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.

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.

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.

As previously discussed with senior agency management, the agency should explicitly take into account the efforts of its Senior Executive Service (SES) members and other responsible staff to address OIG recommendations within their areas of authority in its SES 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. Implementing recommendations 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, mitigate risks to its resources, and support overall agency success.

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. The agency has also made strides in developing an occupant emergency plan and updating its telework guidance. The telework program has proven to be essential in the agency's transition to fulltime telework.

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: Audit of the CPSC's Grants Program, and the Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Audit of the CPSC's Financial Statements for FY 2019, and Risk Assessment of the CPSC's Charge Card Programs.

The statutory audits and reviews related to financial statements, FISMA, and IPERA address this challenge annually. In addition to the statutorily required audits and reviews, the OIG has ongoing work in the areas of the NEISS program, and implementing strategic initiatives in the Office of Communications.

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. This challenge is not unique to the CPSC.

The FY 2019 FISMA evaluation found that management continues to make progress in implementing the FISMA requirements. The CPSC has continued to focus its efforts on the implementation of the following processes/systems:

- Automation of privileged access management for elevated network access
- Development of a formal Enterprise Architecture (EA)
- Engagement with stakeholders in support of the establishment of an Executive Risk function
- Rollout of a role-based training program
- Information Security Continuous Monitoring (ISCM) program
- Documenting and enforcing protocols controlling the destruction/reuse of media containing Personally Identifiable Information (PII) or other sensitive agency data (e.g., proprietary information)
- Enforcement of Personal Identification Verification (PIV) authentication
- Utilization of Simple Mail Transfer Protocol (SMTP) Domain-based Message Authentication, Reporting and Conformance (DMARC) checks
- Enhanced network defense support
- Participation in DHS's EINSTEIN 3 Accelerated program.

The IT challenges currently facing the CPSC are particularly relevant as the agency deals with evolving threats, increasingly sophisticated attacks, new compliance requirements, and the recently identified data breach and unauthorized disclosure of information.

In addition to the hardware and software issues previously identified in OIG reports, the Report of Investigation Regarding the 2019 Clearinghouse Data Breach highlights the need for increased training and oversight regarding the handling of Personally Identifiable Information (PII) and Section 6(b)[3] information. In the past two years there have been multiple instances where the PII and 6(b) information of thousands of people and businesses was either released to unauthorized recipients, transmitted without being properly encrypted, or was accessible to CPSC personnel with no need or authorization to view it. The CPSC moved quickly to notify manufacturers of the release of 6(b) information; however, work remains to be done to address the underlying issues that allowed the releases to occur in the first place.

Over the years this office has identified several security weaknesses in the CPSC's information security internal control policies, procedures, and practices that remain un-remediated. 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 CPSC.

This management challenge aligns with 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 include the: Report of Investigation Regarding the 2019 Clearinghouse Data Breach, Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems, Audit of the CPSC's Financial Statements for FY 2019, and Evaluation of CPSC's FISMA Implementation for FY 2019.

[3] Section 6(b) refers to Section 6(b) of the Consumer Product Safety Act 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.

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, federal data strategy, and the NEISS program.

CONTACT US

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

Call:

301-504-7906
1-866-230-6229

On-line complaint form:

Click here for complaint form.
Click here for CPSC OIG Website.

Write:

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