United States
Consumer Product Safety Commission

Good Accounting Obligation in Government Act Report

The Good Accounting Obligation in Government Act (GAO-IG Act) requires each federal agency, in its annual budget justification, to include a report on:

1. each public recommendation of the Government Accountability Office (GAO) that is designated as "open" or "closed, unimplemented" for a period of at least 1 year preceding the date on which such justification is submitted;
2. each public recommendation for corrective action from the agency's Office of the Inspector General (OIG) that was published at least 1 year before the justification is submitted for which no final action was taken; and
3. the implementation status of each such recommendation.

This report includes GAO and OIG reports issued before February 2023 for which CPSC has open or closed, unimplemented recommendations.

The report has four (4) parts:

Part 1: GAO recommendations and their implementation status.

Part 2: OIG recommendations and their implementation status.

Part 3: Reconciliation of CPSC's records to the OIG's Semi-Annual Report to Congress (SAR) (FY 2022 fall issue).

Part 4: Acronyms

Part 1: GAO recommendations and their implementation status

CPSC has no open GAO recommendations.

Part 2: OIG recommendations and their implementation status

Open OIG Recommendations

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Consumer Product Safety Risk Management System Information Security Review Report	N/A	6/5/2012	Information Technology	1	Identify the participants of the CPSC Risk Executive Council and define specific tasks/milestones for implementing the proposed Risk Management Framework.	Estimated to be complete in FY25
Consumer Product Safety Risk Management System Information Security Review Report	N/A	6/5/2012	Information Technology	2	Develop an Enterprise Architecture that includes a comprehensive IT security architecture using the CIO Council's guidance and incorporate this into the Security Control Documents.	Estimated to be complete in FY25
Consumer Product Safety Risk Management System Information Security Review Report	N/A	6/5/2012	Information Technology	3	Fully document the implementation of the security controls.	Estimated to be complete in FY24
Consumer Product Safety Risk Management System Information Security Review Report	N/A	6/5/2012	Information Technology	4	Update the CPSRMS SSP to be the single authoritative system security document.	Estimated to be complete in FY24
Consumer Product Safety Risk	N/A	6/5/2012	Information Technology	8	Define the specific Public Access controls in place/planned.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Management System Information Security Review Report						
Cybersecurity Information Sharing Act of 2015 Review Report	N/A	8/14/2016	Information Technology	1	Management updates, develops, and publishes general access control and logical access control policies and procedures for all systems that permit access to PII.	Estimated to be complete in FY24
Cybersecurity Information Sharing Act of 2015 Review Report	N/A	8/14/2016	Information Technology	2	Provide training or document training completion by individual system owners on establishing, implementing, and maintaining logical access policies and procedures for systems that contain PII.	Estimated to be complete in FY25
Cybersecurity Information Sharing Act of 2015 Review Report	N/A	8/14/2016	Information Technology	3	The General Access Control Policy and attendant procedures should be updated to include the elements outlined in the report.	Estimated to be complete in FY24
Cybersecurity Information Sharing Act of 2015 Review Report	N/A	8/14/2016	Information Technology	4	Develop, document, and maintain a software inventory including license management policies and procedures.	Estimated to be complete in FY24
Cybersecurity Information Sharing Act of 2015 Review Report	N/A	8/14/2016	Information Technology	5	Comply with and enforce HSPD-12 multifactor authentication supported by the Personal Identity Verification Card.	Estimated to be complete in FY24
Audit of the Telework Program for Fiscal Year 2016	N/A	9/29/2017	Administration of Program Operations	5	Implement a process to validate telework information reported to outside parties and used for internal decision-making to internal source data on a routine basis.	Estimated to be complete in FY24
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	1	Clearly define all the roles to be used in the agency's OEP.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	6	Develop and implement an effective OEP team training program with drills and exercises to include all team members at least annually.	Estimated to be complete in FY24
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	8	Develop and implement procedures to address the needs of individuals requiring additional assistance. These procedures should include a process to routinely update the list of persons requiring assistance.	Estimated to be complete in FY24
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	9	Develop and implement procedures to maintain, retain, and update OEP program documents at least semi-annually.	Estimated to be complete in FY24
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	10	Develop and implement an annual round-table discussion with OEP coordinators and teams.	Estimated to be complete in FY24
Audit of the Occupant Emergency Program for Fiscal Year 2017	18-A-06	6/7/2018	Administration of Program Operations	11	Develop and implement facility-specific policies and procedures.	Estimated to be complete in FY24
Audit of the CPSC's Directives System	19-A-05	3/21/2019	Administration of Program Operations	2	Ensure directives are updated to align with the current directives system policies and procedures as well as reflect the current CPSC organizational structure and operations.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	7	Develop and implement controls to ensure that the data entered into PMS and IFS is accurate and consistent with CPSC policies and procedures.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	8	Develop procedures to review applicable regulations and laws on an annual basis in order to ensure the property management	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
					policies and procedures remain accurate and complete.	
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	9	Perform and document a formal analysis on the PMS operating environment and system mission to determine the appropriate system categorization for PMS.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	10	Upon a justifiable determination of the PMS system categorization, design, implement, and assess the PMS security controls and formally authorize PMS to operate in accordance with CPSC organizational security policies and procedures as well as other applicable government standards.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	11	Establish and implement POA&M management procedures to ensure that all identified security weaknesses, including PMS application-specific and inherited control weaknesses, are fully documented and tracked.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	13	Establish and implement POA&M management procedures to ensure that changes to estimated completion dates should be documented and reflected in the POA&M tracker.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	14	Estimated completion dates should be documented and reflected in the POA&M tracker.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	15	Perform and document a formal analysis of PMS's operating environment and system mission to determine the appropriate risk level categorization for PMS.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	16	Upon a justifiable determination of PMS's system categorization, design and implement standard procedures for requesting and approving user access to roles and resources in PMS.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	20	Perform and document a risk analysis to identify SoD conflicts that may exist between PMS and other CPSC systems.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	21	Upon completion of the risk analysis, develop and implement procedures to ensure that CPSC users do not have unmonitored conflicting access across multiple systems.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	22	Perform and document a risk analysis to identify potential SoD conflicts within PMS.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	23	Upon the completion of the risk analysis noted above, management should develop and implement procedures that ensure PMS users do not have sufficient access to allow the unmonitored execution of incompatible transactions.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	24	Update and implement configuration change management procedures which include requirements to perform and document quality control reviews.	Estimated to be complete in FY24
Review of Personal Property Management System and Practices for Calendar Year 2017	19-A-06	5/31/2019	Administration of Program Operations	25	Develop and implement procedures to log, track, and maintain a list of changes made to the PMS application.	Estimated to be complete in FY24
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	1	Scrub all publicly available documents for any sensitive information.	Estimated to be complete in FY25
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	2	Review existing processes for sanitizing documents and data and ensure employees are aware of these processes.	Estimated to be complete in FY25
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	7	Disable and block unneeded services prior to those systems being placed on the network.	Estimated to be complete in FY24
Report on the Penetration and Vulnerability	19-A-08	6/11/2019	Information Technology	12	Use Microsoft System Center Configuration Manager (SCCM), Group Policy Object (GPO), and endpoint protection software to black list	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Assessment of CPSC's Information Technology Systems					USB Input/Output devices and remove the associated drivers from affected systems.	
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	13	Create a white list of known good USB Input/Output devices and enforce a Bluetooth only policy in regard to wireless accessories.	Estimated to be complete in FY24
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	17	Disable unused Ethernet ports.	Estimated to be complete in FY24
Report on the Penetration and Vulnerability Assessment of CPSC's Information Technology Systems	19-A-08	6/11/2019	Information Technology	20	Ensure that Windows security patches are up to date to prevent the possibility of remotely disabling SMB signing.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	1	Reconvene the BRT to assess the full extent of the breach, and base its response on the totality of the breach.	Estimated to be complete in FY25
Report of Investigation Regarding the 2019 Clearinghouse	20-ROI-01	9/25/2020	Investigation	2	Establish blanket purchase agreements for identity monitoring, credit monitoring, and other related services for data breach victims.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Inadvertent Data Exposure						
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	3	Complete and publish a document describing lessons learned after the BRT completes its work related to this breach.	Estimated to be complete in FY25
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	4	Complete and document annual tabletop exercises. The tabletop exercises test the breach response plan and help ensure that members of the team are familiar with the plan and understand their specific roles. Tabletop exercises should be used to practice a coordinated response to a breach, to further refine and validate the breach response plan, and to identify potential weaknesses in the agency's response capabilities.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	5	Conduct an annual Breach Response Policy plan review.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	6	Establish and complete an annual schedule to review blanket purchase agreements for adequacy, complete and document the tabletop exercise, and publish the updated annual Breach Response Policy plan review.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019	20-ROI-01	9/25/2020	Investigation	12	Review all available data and establish an accurate identification of all data inadvertently	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Clearinghouse Inadvertent Data Exposure					released, internally and externally, from 2010 to 2019.	
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	13	Obtain an independent review of a sample of Clearinghouse responses prior to 2010 to determine the need for an expanded scope of the review.	Estimated to be complete in FY25
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	14	Establish policies and procedures to ensure that when the agency reports data related to a data breach or other violation of law or regulation, the reported data has been independently verified by a person outside of the responsible organization.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	15	Establish a process for communicating and enforcing the implementation of recommendations previously agreed to by management, as required by law.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	17	Implement a single data extraction tool to allow maximum functionality in searching multiple product codes while adequately blocking protected data from release. This tool should default to block ALL fields which may contain 6(b) information and PII data. This data tool must contain a standardized data dictionary to limit placement of restricted information to identified fields.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	18	Once the new tool in Recommendation 17 is implemented, turn off and remove all other data extraction tools from the CPSC inventory of available IT tools.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	19	Limit access to the underlying database and the data extraction tool to those with a bona fide need for access.	Estimated to be complete in FY25
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	22	Annually update and require refresher training for all Clearinghouse staff on the use of the data extraction tool and policies and procedures for accomplishing Clearinghouse work, up to and including the AED for EPHA.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	23	Develop, disseminate, provide training, and implement policies and procedures on how to use this new data extraction tool to all Clearinghouse staff, up to and including the AED for EPHA. These policies must include step-by-step instructions and checklists to aid staff in completing routine tasks. These policies must include guides and checklists for supervisory review of Clearinghouse staff work.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	29	Require initial and annual refresher training for all staff on the importance of protecting 6(b) information and PII, including the rights of individuals and businesses, and how to recognize 6(b) information and PII in	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
					documents and how to securely handle this information.	
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	30	Enforce Principle of Least Privilege and limit access to data on the P-drive to individuals with a bona fide "need to know."	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	32	Determine, document, and implement a structure for the Clearinghouse.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	34	Require the Office of Human Resources Management (Human Resources) to provide consultation to ensure that the organizational structure in EPDSI meets the current operational needs, meets span of control best practices, and perform a skills gap analysis. Human Resources will provide a written report of its findings.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	35	Implement the recommendations from the Human Resources study.	Estimated to be complete in FY24
Report of Investigation Regarding the 2019 Clearinghouse	20-ROI-01	9/25/2020	Investigation	37	Design, document, and implement control activities to respond to the results of the completed risk assessment process.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Inadvertent Data Exposure						
Report of Investigation Regarding the 2019 Clearinghouse Inadvertent Data Exposure	20-ROI-01	9/25/2020	Investigation	38	Develop and implement written guidance on the importance of the statements of assurance process and the related documentation requirements.	Estimated to be complete in FY24
Audit of the CPSC's Office of Communications Management's Strategic Goals	21-A-04	2/19/2021	Administration of Program Operations	10	Implement a risk assessment process to determine where to focus efforts in terms of usefulness and improving message effectiveness.	Estimated to be complete in FY24
Evaluation of the CPSC's Implementation of the Federal Data Strategy	21-A-05	4/16/2021	Information Technology	1	Establish a data strategy implementation project plan with milestones that consider mission priorities and current and expected staffing levels to track the progress of the data management program maturation against the current Data and Analytics Strategy Implementation Plan.	Estimated to be complete in FY25
Evaluation of the CPSC's Implementation of the Federal Data Strategy	21-A-05	4/16/2021	Information Technology	2	Develop and implement a Data Quality Plan that supports the collection and maintenance of data related to identified key CPSC open data sets.	Estimated to be complete in FY25
Evaluation of the CPSC's Implementation of the Federal Data Strategy	21-A-05	4/16/2021	Information Technology	3	Identify and assign responsibilities to all of the resources who have data governance roles and responsibilities. These resources should include, at a minimum, data owners and data stewards, and those resources should be trained on their responsibilities.	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of the CPSC's Implementation of the Federal Data Strategy	21-A-05	4/16/2021	Information Technology	4	Dedicate resources to the data management program based on a needs assessment, which should be revisited as the FDS action plans are published. Supplementary resources to consider adding may include data architects, data scientists, data analysts, and training resources.	Estimated to be complete in FY25
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	1	Update and implement EXRM directives, policies, and procedures regarding position designation to reflect current EXRM operations and address current OPM policies and guidelines.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	2	Develop and maintain an accessible database with all information required to effectively manage the position designation and suitability program. At a minimum, this system should contain the name of the employee or contractor, position number and title, position designation, tier of background investigation completed, entry-on-duty date, date the background investigation was requested, date the background investigation was completed, whether it was an initial investigation or reinvestigation, whether reciprocity was applied, and reinvestigation due date.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	4	Use the information developed in Recommendation Two to track an employee's investigation versus the designation of their position and ensure they are properly aligned.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	5	Use an automated tool to track when employee and contractor reinvestigations are due.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	6	Update the investigations of employees whose completed investigation has exceeded the five-year reinvestigation requirement.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	7	Allocate the appropriate resources going forward to ensure that all reinvestigations are initiated on or before the due date.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	8	Establish a process to include Office of Human Resources Management during the drafting of the statement of work to determine the appropriate investigative tier for contractors prior to when the request for quotes is released to potential vendors.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	9	Develop a formal documented process (directive or standard operating procedure) for onboarding contractors.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	10	Develop a system to communicate any changes in the onboarding process to contracting officer's representatives and other personnel involved in the onboarding of employees and contractors.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	11	Develop and document a systematic and repeatable risk assessment process to evaluate the risk of applying reciprocity for incoming contractors.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	12	Regarding contractors, develop and maintain an accessible database containing the information outlined in Recommendation Two, as well as the contract number, similar CPSC position, contractor name, employer, and name of contracting officer's representative.	Estimated to be complete in FY24
Audit of the CPSC's Position Designation and Suitability Program	21-A-07	4/29/2021	Administration of Program Operations	13	Complete the work required to fully implement OPM's recommendations from 2017.	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	1	Provide guidance identifying programs and/or activities as a part of its internal guidance and in accordance with achieving its mission requirements.	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	2	Align programs and/or activities with applicable reporting requirements.	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	3	Report programs and/or activities in accordance with applicable Federal criteria.	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	4	Provide training to CPSC program managers on how to develop and implement a formal internal controls program in accordance with Standards for Internal Control in the Federal Government, OMB Circular A-123, and CPSC policies and procedures.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	5	Develop a formal internal controls program over operations for CPSC programs.	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	6	Evaluate staffing needs within the Office of Financial Management, Planning and Evaluation to support internal controls and FMFIA reporting requirements	Estimated to be complete in FY24
Audit of the CPSC's Implementation of FMFIA for FYs 2018 and 2019	21-A-08	5/12/2021	Administration of Program Operations	7	Establish formal lines of communication between the Office of Financial Management, Planning and Evaluation and CPSC program management for the purpose of assessing and monitoring internal control programs and compliance with FMFIA requirements.	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	2	Develop, document, and implement a process for determining and defining system boundaries in accordance with the National Institute of Standards and Technology guidance (Risk Management ii/iii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	3	Establish and implement policies and procedures to manage software licenses using automated monitoring and expiration notifications (Risk Management ii/iii).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	4	Establish and implement a policy and procedure to ensure that only authorized hardware and software execute on the agency's network (Risk Management ii/iii).	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	5	Define and document the taxonomy of the CPSC's information system components, and classify each information system component as, at minimum, one of the following types: IT system (e.g., proprietary and/or owned by the CPSC), application (e.g., commercial off-the-shelf, government off-the-shelf, or custom software), laptops and/or personal computers, service (e.g., external services that support the CPSC's operational mission, facility, or social media) (Risk Management ii/iii).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	6	Identify and implement a Network Access Control solution that establishes set policies for hardware and software access on the agency's network (Risk Management ii/iii).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	7	Develop and implement a formal strategy to address information security risk management requirements as prescribed by the National Institute of Standards and Technology guidance (Risk Management iv/v/vi).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	8	Complete an assessment of information security risks related to the identified deficiencies and document a corresponding priority listing to address identified information security deficiencies and their associated recommendations. A corrective action plan should be developed that documents the priorities and timing requirements to address these deficiencies (Risk Management iv/v/vi).	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	9	Develop and implement an Enterprise Risk Management (ERM) program based on the National Institute of Standards and Technology and ERM Playbook (OMB Circular A-123, Section II requirement) guidance. This includes establishing a cross-departmental risk executive (function) lead by senior management to provide both a departmental and organization level view of risk to the top decision makers within the CPSC (Risk Management iv/v/vi).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	11	Develop and implement an information security architecture that supports the Enterprise Architecture. (Risk Management vii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	12	Develop an Enterprise Architecture to be integrated into the risk management process (Risk Management vii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	13	Develop supply chain risk management policies and procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply-chain risk management requirements (Supply Chain Risk Management ii/iii/iv) (2021 recommendation).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	15	Develop and implement a Configuration Management plan to ensure it includes all requisite information (Configuration Management ii/iii).	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	16	Develop, implement, and disseminate a set of Configuration Management procedures in accordance with the inherited Configuration Management Policy which includes the process management follows to develop and tailor common secure configurations (hardening guides) and to approve deviations from those standard configurations (Configuration Management iv/v).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	17	Integrate the management of secure configurations into the organizational Configuration Management process (Configuration Management v).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	18	Consistently implement flaw remediation processes, including the remediation of critical vulnerabilities (Configuration Management vi).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	19	Identify and document the characteristics of items that are to be placed under Configuration Management control (Configuration Management vii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	20	Establish measures to evaluate the implementation of changes in accordance with documented information system baselines and integrated secure configurations (Configuration Management vii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	21	Define and document a strategy (including specific milestones) to implement the Federal Identity, Credential, and Access Management	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
					architecture (Identity and Access Management i/ii/iii).	
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	22	Integrate Identity, Credential, and Access Management strategy and activities into the Enterprise Architecture and Information System Continuous Monitoring (Identity and Access Management i/ii/iii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	23	Develop, formalize (through the CPSC's D-100 process), and implement processes to ensure all personnel are assigned risk designations and appropriately screened prior to being granted access to agency systems. Prior to formalizing the existing risk designation procedures, these procedures should be enhanced to include the following requirements: • Performance of periodic reviews of risk designations at least annually, • Explicit position screening criteria for information security role appointments, and • Description of how cybersecurity is integrated into human resources practices (Identity and Access Management iv).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	24	Define and implement a process to ensure the completion of access agreements for all CPSC users. (Identity and Access Management v).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	26	Identify and document potentially incompatible duties permitted by privileged accounts (Identity and Access Management vii).	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	29	Log and actively monitor activities performed while using privileged access that permit potentially incompatible duties (Identity and Access Management vii).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	30	Define and implement the identification and authentication policies and procedures (Identity and Access Management ii).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	31	Define and implement processes for provisioning, managing, and reviewing privileged accounts (Identity and Access Management vii) (2021 recommendation).	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	32	Document and implement a process for inventorying and securing systems that contain Personally Identifiable Privacy) Information or other sensitive agency data (e.g., proprietary information) (Data Protection and Privacy i).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	33	Document and implement a process for periodically reviewing for and removing unnecessary Personally Identifiable Information from agency systems (Data Protection and Privacy i).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	35	Identify all CPSC personnel that affect security and privacy (e.g., Executive Risk Council, Freedom of Information Act personnel, etc.) and ensure the training policies are modified to require these individuals to participate in role-based security/privacy training (Data Protection and Privacy iii).	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	36	Perform an assessment of the knowledge, skills, and abilities of CPSC personnel with significant security responsibilities (Security Training i).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	37	Document and implement a process for ensuring that all personnel with significant security roles and responsibilities are provided specialized security training to perform assigned duties (Security Training ii/iii) (2021 recommendation).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	38	Develop and tailor security training content for all CPSC personnel with significant security responsibilities and provide this training to the appropriate individuals (Security Training iv/v).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	39	Integrate the established strategy for identifying organizational risk tolerance into the Information System Continuous Monitoring plan (Information System Continuous Monitoring i).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	40	Implement Information System Continuous Monitoring procedures, including those procedures related to the monitoring of performance measures and metrics, that support the Information System Continuous Monitoring program (Information System Continuous Monitoring ii) (2021 recommendation).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	45	Develop, document, and distribute all required Contingency Planning documents (e.g.. organization-wide Continuity of Operation Plan	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
					and Business Impact Assessment, Disaster Recovery Plan, Business Continuity Plans, and Information System Contingency Plans) in accordance with appropriate federal and best practice guidance (Contingency Planning ii/iv).	
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	46	Integrate documented contingency plans with the other relevant agency planning areas (Contingency Planning iii).	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2021	22-A-01	10/29/2021	Information Technology	47	Test the set of documented contingency plans (Contingency Planning iv).	Estimated to be complete in FY25
Evaluation of the CPSC's NIST Cybersecurity Framework Implementation	22-A-04	1/18/2022	Information Technology	1	Complete a National Institute of Standards and Technology (NIST) Cybersecurity Framework current profile in accordance with NIST guidance.	Estimated to be complete in FY25
Evaluation of the CPSC's NIST Cybersecurity Framework Implementation	22-A-04	1/18/2022	Information Technology	2	Conduct an assessment to identify the highest risks to the CPSC's security profile based on the information learned while completing the National Institute of Standards and Technology Cybersecurity Framework current profile exercise.	Estimated to be complete in FY25
Evaluation of the CPSC's NIST Cybersecurity Framework Implementation	22-A-04	1/18/2022	Information Technology	3	Complete a National Institute of Standards and Technology Cybersecurity Framework (NIST) target profile in accordance with NIST guidance.	Estimated to be complete in FY25
Evaluation of the CPSC's NIST Cybersecurity Framework Implementation	22-A-04	1/18/2022	Information Technology	4	Perform an assessment to identify gaps between the current and target National Institute of Standards and Technology Cybersecurity Framework profiles.	Estimated to be complete in FY25

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
Evaluation of the CPSC's NIST Cybersecurity Framework Implementation	22-A-04	1/18/2022	Information Technology	5	Update and implement the CPSC Framework Implementation Action Plan.	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2022	22-A-06	7/22/2022	Information Technology	1	Implement registration and inventorying procedures for the CPSC's information systems.	Estimated to be complete in FY24
Evaluation of CPSC's FISMA Implementation for FY 2022	22-A-06	7/22/2022	Information Technology	10	Implement solutions to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data.	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2022	22-A-06	7/22/2022	Information Technology	17	Implement data encryption and sanitization of digital media policies and procedures.	Estimated to be complete in FY25
Evaluation of CPSC's FISMA Implementation for FY 2022	22-A-06	7/22/2022	Information Technology	20	Update the System Security Plans to include the most up-to date information and assess the relevant minor applications.	Estimated to be complete in FY25
CPSC Penetration Test 2022	23-A-02	12/13/2022	Information Technology	3	Use a client-side JavaScript to verify that the user confirms their password before proceeding with the reset process. Moreover, password confirmation should also be performed on the server-side to complete the reset process.	Estimated to be complete in FY24
CPSC Penetration Test 2022	23-A-02	12/13/2022	Information Technology	6	Upgrade the recalls.gov and saferproducts.gov web applications to the latest version of the jQuery and VUE.	Estimated to be complete in FY24

Report Title	Report Number	Issue Date	Audit Area	Rec #	Recommendation	Implementation Status
CPSC Penetration Test 2022	23-A-02	12/13/2022	Information Technology	7	Configure FOIAPAL to require users to change their password upon their first login as a best practice.	Estimated to be complete in FY24
CPSC Penetration Test 2022	23-A-02	12/13/2022	Information Technology	10	Disable Link-Local Multicast Name Resolution and NetBIOS Name Service through a Group Policy or manually if necessary.	Estimated to be complete in FY24
CPSC Penetration Test 2022	23-A-02	12/13/2022	Information Technology	11	Enable the 'require pass' directive in the redis.conf configuration file.	Estimated to be complete in FY24

Part 3: Reconciliation of CPSC's records to the OIG's Semi-Annual Report to Congress (SAR) FY 2022 Fall issue

	GAO-IG Act Report	SAR (September 2023 Issue)
Reporting Criteria	As required by the GAO-IG Act, this report includes recommendations that remain unimplemented for one year or more from the budget justification submission date. This report includes recommendations that were issued on or before 1/30/2023 and remained unimplemented as of 1/30/2024.	As required by the Inspector General Empowerment Act of 2016, the SAR includes recommendations that remained unimplemented for six months or more from the SAR reporting end date. The September 2023 SAR had a reporting end date of 9/30/2023, and therefore includes recommendations that remained unimplemented since their issuance on or before 3/31/2023.
Total Open Recommendations	A total of 136 recommendations with a status of *open*.	A total of 178 recommendations with a status of *open*.

Part 4: Acronyms

Acronym	Description
6(b)	Section 6(b) of the Consumer Product Safety Act
AED	Associate Executive Director
BRT	Breach Response Team
CIO	Chief Information Officer
CPSC	Consumer Product Safety Commission
CPSRMS	Consumer Product Safety Risk Management System
DCM	Dynamic Case Management System
EPHA	Division of Hazard Assessment
EPDSI	Division of Data Systems
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
HSPD-12	Homeland Security Presidential Directive 12
IDI	In-Depth Investigation
IFS	Integrated Field System
IT	Information Technology
NEISS	National Electronic Injury Surveillance System
OCM	Office of Communications
OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
OPM	Office of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMS	Property Management System
POA&M	Plan of Action and Milestones
SMB	Server Message Block
SoD	Separation of Duties
SOP	Standard Operating Procedure
SSP	System Security Plan
VGB	Virginia Graeme Baker Pool and Spa Safety Act