FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

ANNUAL REPORT
FISCAL YEAR 2023

Note

The Office of Management and Budget (OMB) is publishing this report in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, sec. 2(a), § 3553(c) (codified at 44 U.S.C. § 3553(c)). This report also incorporates OMB's analysis of agency application of intrusion detection and prevention capabilities, as required by the Cybersecurity Act of 2015, Pub. L. No. 114-113, § 226(c)(1)(B), and agency reporting on compliance with privacy requirements and management of privacy risks.

OMB obtained information from the Department of Homeland Security (DHS), agency Chief Information Officers (CIOs), Inspectors General (IGs), and Senior Agency Officials for Privacy (SAOPs) from across the Executive Branch to compile this report. This report primarily includes Fiscal Year 2023 data reported by agencies to OMB and DHS.

Table of Contents

Executive Summary: A Zero Trust Foundation

Spurred by President Biden's issuance of Executive Order 14028, *Improving the Nation's Cybersecurity* (EO 14028), in May 2021, the Federal Government has made significant progress towards realizing the vision to "foster a more secure cyberspace" by making "bold changes and significant investments in order to defend the vital institutions that underpin the American way of life." In Fiscal Year (FY) 2023, the Administration continued to make progress in both implementing key cybersecurity protections, such as endpoint detection and response (EDR) and multi-factor authentication (MFA), and measuring agencies' maturity in achieving the goals in EO 14028. Automating the collection of agency data facilitates the measurement of agencies' progress, alleviating manual data entry burdens and allowing agencies to focus time and resources on meaningful security outcomes.

In FY 2023, the Office of Management and Budget (OMB) worked to further institutionalize and embed zero trust principles across the Federal enterprise. Agencies are now positioned to achieve specific zero trust security goals by the end of FY 2024, as required by OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. OMB has also regularly engaged with the Office of the National Cyber Director (ONCD) to promote a comprehensive vision of cybersecurity that recognizes how essential cybersecurity is to "the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."[1]

To that end, in March 2023 the Administration released the National Cybersecurity Strategy (NCS), which calls for the modernization Federal defenses and serves as a blueprint to a more secure future. To date, the Federal government has largely proven successful in meeting the deadlines outlined in the NCS Implementation Plan (NCSIP).

To ensure Federal agencies are prioritizing efforts and resources to achieve the goals laid out in EO 14028, subsequent OMB memoranda, and the NCS, OMB and ONCD jointly issued OMB Memorandum M-23-18, *Administration Cybersecurity Priorities for the FY 2025 Budget.* This document outlines the Administration's cyber investment priorities and provides guidance to agencies on areas of emphasis for formulating their FY 2025 budget proposals.

Taken together, these actions are cementing the Federal Government's shift to a new cybersecurity paradigm that aims to dramatically reduce the risk of successful cyber-attacks against our digital infrastructure.

Privacy and cybersecurity are separate but related disciplines, making coordination critical. Therefore, this report also reflects agencies' reporting on their privacy performance through their responses to the Senior Agency Official for Privacy (SAOP) metrics.

---

[1] National Cybersecurity Strategy (Mar. 2023).

FY 2023 Report Key Takeaways:

The FISMA Metrics Subcommittee was launched in FY 2023 to coordinate and collaborate on FISMA CIO metrics.
FMSC members provide constructive feedback on FISMA metrics, which increases agency engagement and leads to more effective and meaningful metrics.

Agencies show improvements in adoption of cyber defensive measures.
Every agency has selected an enterprise EDR platform for their agency in accordance with OMB Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*.

Agencies are expanding their cyber detection capabilities.
96 percent of Federal civilian Executive branch agencies recorded an increase in the Detect category in FY 2023 as compared to FY 2022.

Section I: Federal Cybersecurity Activities

A. Maturation Towards a Zero Trust Architecture

Institutionalizing Zero Trust Architecture: EO 14028 and the NCS

EO 14028 was issued in May 2021 by the Biden Administration as a bold call to action to modernize Federal cybersecurity defenses, improve information-sharing between the Federal Government and the private sector on cyber issues, and strengthen agencies' ability to respond to incidents when they occur.

These goals were especially important in FY 2023, as agencies are required to complete a number of EO 14028-related actions by the end of FY 2024. OMB has continued to support and advance agency adoption of EO 14028-related actions by: measuring and sharing progress made to date with the public and agency leadership; supporting budget priorities that assist agencies in achieving EO 14028 goals; and sponsoring working groups and workshops to aid in implementation.

In collaboration with OMB, the CyberStat program at the Cybersecurity and Infrastructure Security Agency (CISA) hosted 11 workshops focused on zero trust implementation. Zero trust-focused CyberStat workshops addressed the zero trust maturity model, operational visibility, and data, among other items. CyberStat workshops are designed to provide agencies with the necessary support, guidance, and access to resources to assist them in implementing the actions directed by EO 14028 and OMB circulars and memoranda. These workshops drew several thousand Federal IT professional attendees from across the government.

As in past years, OMB continued to track Federal agencies' progress toward zero trust goals through CIO FISMA metrics. FY 2023 marked a dramatic change in the way metrics were selected and how data were collected. The Chief Information Security Council, in coordination with OMB, launched the FISMA Metrics Subcommittee (FMSC) to better collaborate with agencies on CIO FISMA metrics. FMSC members provided constructive feedback on CIO FISMA metrics, increasing agency engagement and highlighting possible ways to build more effective and meaningful metrics.

Increased use of automation improved the collection of data for FISMA metrics. Data collection for metrics regarding assets and vulnerabilities was automated. Automated collection reduces the administrative burden on agencies, allowing cybersecurity personnel to spend less time reporting and more time on high-impact cyber risk reduction activities. Where fully automated collection is not yet achievable, CISA is providing performance and incident data to OMB in an automated manner and machine-readable format. This effort now allows OMB to develop analysis and oversight toolsets that support the White House's drive for a secure Federal enterprise.

In FY 2023, consistent with prior years, agencies were measured on their maturation in the five functions of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). CIO FISMA metrics continued to reflect agencies' progress in institutionalizing EO 14028 goals. The metrics include data on percentage of devices scanned within given timeframes; EDR platforms; and per M-22-09, removal of password policies that require special characters, among other

capabilities and activities. OMB gauges the maturity of agencies' cybersecurity programs and practices by assigning points to the various FISMA metrics. An agency that achieved the best possible result on all metrics would score a 100. In FY 2022, only one agency scored above 90. In FY 2023, 12 did so.

OMB published the [Federal Cybersecurity Progress Report](#) twice in FY 2023 to provide the public with a precise, fair, and comprehensive assessment of agency cybersecurity posture. OMB will continue overseeing Federal agencies' implementation of Administration cybersecurity policies through CIO FISMA metrics.

B. Program and Policy Areas

Continued Progress on the Federal Zero Trust Strategy

Since the release of M-22-09 in May 2022, Federal agencies have demonstrated tangible progress in implementing zero-trust initiatives. Quantitative metrics cannot fully show how agencies have undergone a culture change that embraces zero trust methodologies; this has been drawn out through interviews and qualitative questionnaires. These efforts found agencies have chosen priorities based on their own risk profiles to achieve core zero trust principles. Quantitative data did show that agencies are making notable progress in the deployment of MFA at the application layer and the adoption of enterprise identity solutions. Agencies have also reported an improvement in their incident response capabilities. Encryption of data both at rest and in transit also continues to advance. There is also rapid and widespread deployment of EDR capabilities across the Federal enterprise. And, in an effort to ensure greater coordination and visibility, every agency has worked with CISA to select and deploy an enterprise EDR platform as necessary. Agencies have also improved their ability to capture, analyze, or store logs, and the quality of collected logs has improved.

A paradigm shift to zero trust requires continuing investments in modern cybersecurity practices and technologies. Where challenges exist, policies such as OMB Memorandum M-23-18, *[Administration Cybersecurity Priorities for the FY 2025 Budget](#)* (M-23-18), co-signed by OMB and ONCD, will assist in ensuring continued future progress. By aligning to the NCS, agencies can continue to modernize their security infrastructure and deliver large scale impact.

To continue to accelerate agency progress on zero trust, OMB has laid the groundwork for agencies to draw upon the expertise of both other agencies and the best minds in industry. In FY 2022, OMB established the Identity Credentialing and Access Management Community of Action focused on the deployment of industry-leading technical capabilities for authentication. OMB launched a second cohort in FY 2023 to help more agencies deploy modern authentication solutions. Also, in FY 2023, CISA, in coordination with OMB, launched the Protective Domain Name Service (DNS) Community of Action.

Continuous Diagnostics and Mitigation (CDM) and the National Cybersecurity Protection System (NCPS)

Both the Continuous Diagnostics and Mitigation (CDM) program and the National Cybersecurity Protection System (NCPS) are CISA-led programs designed to assist Federal agencies in enhancing their cybersecurity posture. The CDM program was established in 2012 and provides risk-based,

consistent, and cost-effective commercial-off-the-shelf (COTS) cybersecurity solutions to protect Federal systems across all organizational tiers. Similarly, the National Cybersecurity Protection System (NCPS) provides a suite of tools to enhance the boundary awareness and security of Federal agencies. NCPS is structured around five capability areas: Intrusion Detection; Intrusion Prevention; Analytics; Information Sharing; and Core Infrastructure. NCPS Intrusion Prevention services ended in December 2023. NCPS capabilities are complemented by other systems and tools inside agency networks that are provided through mechanisms such as CDM. These two programs work collaboratively to enhance situational awareness, analysis, and incident response across Federal networks.

The CDM program supports Federal agencies' ability to prioritize cybersecurity risks, enabling mitigation of the most significant problems first. The CDM program also provides CISA with a near real-time view of the Federal enterprise cyber threat landscape through the Federal CDM dashboard, which receives summary data from all Federal agency dashboards. CDM objectives are to reduce agency-specific security threats, increase visibility into the Federal enterprise cybersecurity posture, improve Federal cybersecurity response capabilities, and streamline reporting pursuant to FISMA. In FY 2023, CDM began reporting certain FISMA metrics automatically on behalf of agencies through their CDM Dashboards. This automated reporting has enhanced coordination amongst agencies, OMB, and CISA while reducing manual effort and human error and improving security and visibility. CDM intends to work with OMB to increase the number of metrics reported automatically through the Dashboard in FY 2024, further benefiting agencies.

Through funding made available from the American Rescue Plan Act in FY 2021, CISA began acquiring EDR tools for 54 agencies, including both Chief Financial Officer (CFO) Act agencies (14 agencies) and non-CFO Act agencies (40 agencies). As of the end of FY 2023, there are 76 agencies that have met a threshold of at least 80 percent coverage of known endpoints with their EDR solution, either independently (40 agencies) or with CISA's assistance (36 agencies).

Through the end of FY 2023, the CDM program made significant progress in addressing known gaps and operationalizing enterprise EDR solutions in support of the goals of EO 14028:

- Procured 1.2 million EDR licenses to close agency identified gaps;
- Deployed over 750,000 EDR licenses across 54 agencies;
- Completed deployment efforts with 36 agencies;
- Onboarded 36 agencies into CISA's Persistent Access Capability (PAC) to enable continuous threat hunting activities; and
- Completed the first phase of Host Level Visibility (HLV) rollouts.

CDM continued efforts to improve visibility and strengthen protections for mobile devices:

- Completed Enterprise Mobility Management (EMM) integration at 15 agencies (five CFO Act Agencies, 10 non-CFO Act agencies);
- Expanded EMM deployments to include an additional ten agencies (six CFO Act, four non-CFO Act); and
- Integrated mobile asset management data into the CDM Dashboard for seven agencies.

Additionally, the CDM Program expanded identity management deployments to support 16 CFO Act agencies and 3 non-CFO Act agencies and released the last major platform update to the CDM Dashboard capability to support visibility improvements and rapid content updates.

Similar to the CDM program, CISA's NCPS provides a suite of tools to enhance the boundary awareness and security of Federal agencies. As previously noted, NCPS is structured around five capability areas: Intrusion Detection (EINSTEIN 1 (E1), EINSTEIN 1 Enhanced (E1E), EINSTEIN 2 (E2)); Intrusion Prevention (EINSTEIN 3 Accelerated (E3A)); Analytics; Information Sharing; and Core Infrastructure.

In FY 2023, the Department of Homeland Security (DHS) approved the establishment of a new program – the Cyber Analytic and Data System (CADS). CADS builds upon prior investments in the NCPS infrastructure, analytics, and information sharing capability areas to establish a foundational environment to support CISA cyber operations. CISA continues to make progress deploying new technologies and entering into new agreements that provide unprecedented visibility into cyber threats affecting American networks. CADS will provide a modern, scalable, and unclassified analytic infrastructure for CISA's cyber operators and aligns with the vision of CISA's Joint Collaborative Environment. CADS is being established to provide the mission infrastructure, analytic tools, and engineering expertise to integrate formerly stove-piped data sets, offer a common set of data management and analytic tools, and provide the agility to scale and evolve over time in support of mission requirements. CADS will focus exclusively on meeting the operational demands of CISA cybersecurity operators, analysts, and decision makers to better protect and serve their stakeholder communities, to include the Federal, state, local, tribal, and territorial (SLTT) government entities, critical infrastructure, private sector companies, and the public.

As part of this transition, NCPS activities in FY 2023 focused on expanding the analytic environment infrastructure to support new operational visibility datasets, developing a data integration roadmap, continuing migration of on-premise capabilities to the cloud analytic environment, and implementing additional analytic tools to support the new datasets available to CISA cyber operators. CISA has made considerable progress towards these transition goals; 89 percent of tools were migrated as of FY 2023 Q4, and a data ingest/integration roadmap has been developed. Further, as the Federal Government shifts away from perimeter-based defenses and adopts a zero trust architecture, data from capabilities like EDR will be integrated into the CADS analytic environment to allow our cyber defenders to automate certain protections, as well as quickly detect and mitigate malicious activity.

Intrusion Prevention and Intrusion Detection services (otherwise referred to as the EINSTEIN sensor suite) are not in scope of the CADS program. As planned, EINSTEIN 3 Accelerated (E3A) Intrusion Prevention services, both DNS Sinkholing and Email Filtering, were retired in December 2023. CISA's Protective DNS capability, a state-of-the-art recursive DNS resolver service, replaces the E3A DNS Sinkholing capability and prevents government internet traffic from reaching known malicious destinations. E3A Email Filtering Service has not been replaced by a new CISA service, as CISA recognizes that most agencies have adopted highly effective commercial email filtering capabilities that meet or exceed those provided by the E3A Email Filtering Service.

Table 1 demonstrates NCPS implementation status as of September 30, 2023. Future iterations of this report may include updates on the transition away from EINSTEIN services to CADS as outlined above.

Table 1 NCPS Intrusion Detection and Prevention Capabilities Implementation Summary for Federal Civilian Agencies

EINSTEIN Capability	Complete		In Progress		Deferred		Not Implemented	
Fiscal Year	**2022**	**2023**	**2022**	**2023**	**2022**	**2023**	**2022**	**2023**
E1/E2	**85**	**85**	**1**	**1**	**0**	**0**	**18**	**18**
CFO	23	23	0	0	0	0	0	0
Non-CFO	62	62	1	1	0	0	18	18
E3A Email	**85**	**85**	**0**	**0**	**5**	**0**	**14**	**19**
CFO	23	23	0	0	0	0	0	0
Non-CFO	62	62	0	0	5	0	14	19
E3A DNS	**79**	**36**	**0**	**0**	**0**	**0**	**15**	**0**
CFO	19	1	0	0	0	0	0	0
Non-CFO	60	35	0	0	0	0	15	0
Protective DNS	**10^2**	**66**		**26**		**0**		**12^3**
CFO	4	22		1		0		0
Non-CFO	6	44		25		0		12

---

[2] The FY 2022 figure for Protective DNS "Complete" indicates the number of agencies that were participating in the Protective DNS beta service, prior to general availability.

[3] Twelve Non-CFO Act agencies did not implement E3A DNS. Protective DNS will be implemented/deployed at those agencies in FY 2024.

Vulnerability Disclosure Policies and Programs

Vulnerability disclosure policies (VDP) enable agencies to improve their information security programs by welcoming cybersecurity review from external researchers. VDPs allow agencies to obtain new insights into security vulnerabilities and understand the agency's external risk posture, which provides a high return on investment. VDPs also provide protection for those who uncover these vulnerabilities by explicitly authorizing good-faith security research. In FY 2023, all CFO Act agencies other than the Department of Defense[4] reported having a VDP. Of those agencies, all but one had a VDP that covered either all internet-accessible or Federal information systems, and many had a VDP that also permitted reporting on internally-facing Federal systems.

High Value Assets

The CISA High Value Assets (HVA) program plans, prioritizes, and coordinates delivery of cybersecurity services to assist Federal agencies in identifying, managing, and assessing their respective HVAs to better enable the identification and risk assessment of the overall Federal HVA enterprise. HVA assessments collaboratively evaluate the risk management posture of an HVA.

Agencies may designate Federal information or information system as an HVA when it relates to one or more of the following categories:[5]

- *Informational Value* – The information or information system that processes, stores, or transmits the information is of high value to the Federal Government or its adversaries.
- *Mission Essential* – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions, as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
- *Federal Civilian Enterprise Essential* – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

All agencies are responsible for the ongoing authorization of their information systems to ensure the accuracy of information pertaining to the security and privacy posture of their HVAs. HVA assessments are critical to maintaining an unbiased view of the risk associated with maintaining an HVA. Agencies are therefore required to ensure HVA assessments are conducted in accordance with OMB and CISA requirements.[6]

During the COVID-19 pandemic, Federal agencies expanded the availability of telework to employees and contractor personnel and limited the number of staff allowed into Federal government buildings and facilities. Consequently, CISA faced challenges conducting Security Architecture Reviews (SAR) and Risk and Vulnerability Assessments (RVA) each requiring individual visits. To address this issue and to avoid backlogs, CISA's HVA Program Management Office revised the assessment process by

---

[4] The Department of Defense submits FISMA metrics and additional data on agency progress towards the deployment of advanced cybersecurity capabilities and programs through their classified cybersecurity scorecard and thus are not included in this analysis.

[5] OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program* (M-19-03).

[6] M-19-03; CISA Binding Operational Directive 18-02.

combining the SAR and RVA into a single methodology. Using this methodology in FY 2023, agency HVA assessments continued to identify the challenges Federal agencies face in mitigating security vulnerabilities on these critical assets. The most common security deficiencies identified across the HVA landscape are identified in Figure 1.

In FY 2023, CISA conducted 37 total HVA assessments resulting in 349 findings. Put another way, in FY 2023 there were 9.4 findings per visit, keeping pace with the per-visit findings from FY 2022. Patch management remains the top finding as it has for each fiscal year since FY 2021. As in prior years, agencies in FY 2023 submitted patching data as part of their FISMA metrics to reveal how well agencies are prioritizing and applying patches within the enterprise.

Figure 1 Top 5 High Value Asset Assessment Findings in FY23

1	Patch Management
2	Unsupported OS or Application
3	Authentication Bypass
4	Defense in Depth
5	Insecure Group Policy Preferences

Unsupported OS or application remains consistent with FY 2022 as the second most prevalent finding; prior to FY 2022, this finding had not appeared on the top-five list since FY 2017. To better monitor agencies' modernization progress, FY 2023 CIO FISMA metrics require agencies to report data on End of Life, End of Service and extended support software. Authentication bypass (e.g., weak passwords, admin password re-use) was the third most typical finding, as in FY 2022. This finding has been consistent since FY 2017 and continues to remain a significant concern. Defense in depth and insecure group policy preferences remained in the top five for FY 2023.

Binding Operational Directives and Emergency Directives

The Federal Information Security Modernization Act of 2014 authorizes DHS, in coordination with OMB, to develop and oversee the implementation of cybersecurity Binding Operation Directives (BODs) and Emergency Directives (EDs), which require Federal agencies to take action in order to comply with the directives. BODs address agency implementation of OMB policies, principles, standards, and guidelines. EDs address known or reasonably suspected information security threats, vulnerabilities, and incidents that represent a substantial threat to agencies.

CISA leads DHS efforts to develop, communicate, and manage actions and critical activities related to all directives, in close coordination with OMB. DHS issued two BODs in FY 2023:

- BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks: Released on October 3, 2022, BOD 23-01 required two core activities to improve operational visibility: asset discovery and vulnerability enumeration. The goal of BOD 23-01 was for agencies to achieve the following outcomes: maintain an up-to-date inventory of networked assets; identify software vulnerabilities; track the frequency and coverage of asset enumeration and the currency of vulnerability signatures; and provide asset and vulnerability

information to CISA's CDM Federal Dashboard. Agencies are required to adhere to the timelines set forth in the CISA-managed vulnerability catalog and report on the status of vulnerabilities listed in the repository.

- BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces: On June 13, 2023, CISA issued BOD 23-02, requiring Federal agencies to take steps to reduce the risk from internet-exposed network interfaces. The directive requires agencies to remove networked management interfaces from the internet and/or protect those interfaces by deploying zero trust capabilities that enforce access control to the interface through a policy enforcement point separate from the interface itself. Agencies are also required to implement technical and/or administrative controls to ensure that all newly added as well as all existing network devices identified by the scope of this directive have (a) the management interface removed from being internet facing and/or are (b) configured with a zero trust architecture design.

# Section II: Federal Cybersecurity Reporting and Analysis

OMB leverages data as a strategic asset to increase the effectiveness of the Federal Government, facilitate oversight, and promote transparency. To this end, OMB publishes a portion of the collected data to the public; this section of the report includes findings based on those data.

A. Tracking Progress in Zero Trust Architecture Adoption

Cybersecurity Progress Report

OMB evaluates agency-submitted data to conduct oversight of agency information security policies and practices. In FY 2023, OMB used the CIO FISMA metrics to track agency progress in implementing EO 14028 and subsequent policy guidelines. To show agency progress, OMB published Federal Cybersecurity Progress Reports on performance.gov for both the second and fourth quarters of FY 2023. Progress reports provide the public and stakeholders with precise, fair, and comprehensive assessments of the cybersecurity posture of all CFO Act agencies except the Department of Defense—a total of 23 agencies.[7] Data derived from agency responses to annual CIO FISMA Metrics are grouped into five categories, aligning with NIST's Cybersecurity Framework (CSF): Identify, Protect, Detect, Respond, and Recover.

Figure 2 Federal Cybersecurity Progress Report

Composite Score	No. of Agencies
🟢 90-100	12
🟩 80-89	7
🟡 70-79	4
🟠 60-69	0
🔴 <59	0
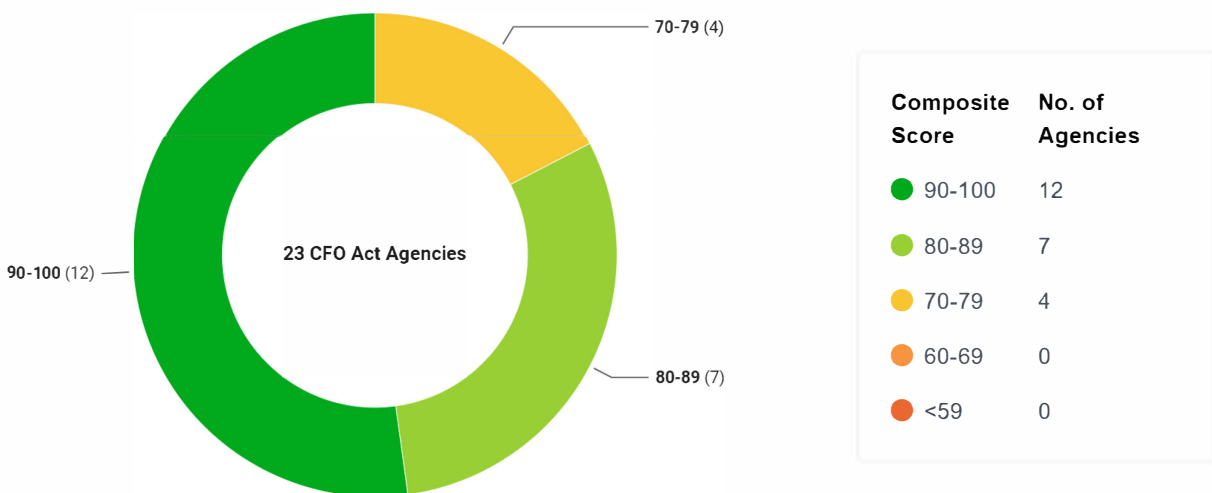
The average score among the 23 CFO Act agencies was 87 (out of a possible 100), a six percent increase from FY 2022; 12 agencies received a score greater than 90; seven agencies received scores between 80-89; and four agencies received scores between 70-79. Of the five CSF categories, major

---

[7] The Department of Defense submits FISMA metrics and additional data on agency progress towards the deployment of advanced cybersecurity capabilities and programs through their classified cybersecurity scorecard.

gains compared to FY 2022 scores were observed in the Protect and Detect categories. The Protect category measured agencies' progress in encryption, MFA, and smart patching. The Detect category measured agencies' progress in conducting penetration testing, red team exercises, HVA assessments, and VDP program implementation.

Agencies continue to execute key Administration cybersecurity priorities to reduce risk to the Federal Government. Progress reports also make clear that large-scale change as envisioned in EO 14028 requires continued investment, collaboration, and cultural change. To continue to drive systemic security change across the Federal enterprise, OMB will continue measuring agencies' progress as they adapt to meet ever-rising expectations of agency cybersecurity operations.

Independent Assessments

FISMA requires an agency's inspector general (IG), or an independent external auditor[8] to conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. [9] Each year these independent assessors report on metrics (IG FISMA Metrics)[10] developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) in coordination with OMB, DHS, the Federal CIO Council, and other stakeholders. Each metric and each function of the NIST Cybersecurity Framework is assessed using a five-level maturity model.

Pursuant to OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements,* and the IG FISMA Metrics, OMB believes that a finding of *Managed and Measurable* (Level 4) is considered to be effective at the domain, function, and overall levels. To provide IGs with greater flexibility to evaluate the maturity of their agencies' cybersecurity programs in the context of their unique missions, resources, and challenges, the IG FISMA Metrics provide IGs with the discretion to rate their agencies as effective below the *Managed and Measurable* level. However, OMB strongly encourages IGs to use the five-level maturity model to determine the effectiveness of their agencies' cybersecurity programs.

In FY 2023, OMB implemented a new framework for both the timing and focus of IG assessments. The goal of the new framework is to provide more flexibility but continued focus on annual assessments for the Federal community. This effort yielded two distinct groups of metrics, Core and Supplemental.

- **Core Metrics:** Metrics that are assessed annually and represent a combination of Administration priorities, high impact risk reduction activities, and essential functions necessary to determine security program effectiveness.
- **Supplemental Metrics:** Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

IGs were instructed to evaluate both Core and Supplemental Metrics in FY 2023. Agencies are focusing and improving on Core Metrics across the board. Of the 20 Core Metrics, agencies improved in 18. This

---

[8] 44 USC § 3555(b).

[9] 44 USC § 3553(c)(3) requires that this report include a summary of these independent evaluations; the summary for each agency can be found in its one-pager.

[10] The FY 2023-2024 IG FISMA Metrics are available at CISA's website.

improvement shows agencies' dedication to implementing priorities. Agencies did see a downward trend in Core Metrics focused on incident detection and analysis and defining roles and responsibilities associated with change control management.

Agencies have continued to make considerable progress in Supply Chain Risk Management (SCRM) activities since the addition of that topic to the IG FISMA Metrics in FY 2021. The continued improvement in SCRM is notable, and additional work will further that progress.

Table 2 shows the number of agencies assessed as having an effective information security program from FY 2019 to FY 2023. CFO Act agencies have improved over time in developing effective security programs.

Table 2 IG Information Security Effectiveness Ratings

	Agency Type	FY19	FY20	FY21	FY22	FY23
Number of agency information security programs rated as overall "Effective"	CFO	5	7	5	8	8
	Non-CFO	40	45	50	43	43
	Total	45	52	55	51	51

B. FY 2023 Information Security Incidents

Agencies are required to report information security incidents to CISA in accordance with CISA's Incident Notification Guidelines. Incidents that must be reported include events that have been under investigation for 72 hours without successful determination of their root cause or nature (i.e., malicious, suspicious, or benign). As required under FISMA, this report provides summary information on the number of cybersecurity incidents that occurred across the Federal Government.

Over the course of FY 2023, 32,211 incidents were reported by Federal agencies, which represents a 9.9 percent increase from the 29,319 incidents reported in FY 2022. These additional incidents were mostly considered "Minor" events under the National Cyber Incident Scoring System (NCISS). Minor events are "[h]ighly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence." (See Table 4, *Agency-Reported Incidents by NCISS Priority Level*). In total, there was an increase of 5,396 minor incidents reported to CISA.

Generally, agencies cited improved detection capabilities at Security Operations Centers (SOCs), additional automation and training, and changes in event and incident tracking methodologies as the primary reasons for the increase in incidents over the past fiscal year.

US-CERT Incidents by Vector

Agencies must classify incidents by method of compromise or data loss as part of their reporting requirements.[11] These data provide visibility into the threats agencies face every day, allowing for a better understanding of the risks to Federal systems and data.

Table 3, "Agency-Reported Incidents by Attack Vector," identifies the number of incidents reported by Federal agencies across nine categories. For FY 2023, the "Improper Usage" vector accounted for the highest number of reported incidents – 12,261, or roughly 38 percent of total incidents. This data suggests that although agencies have processes or capabilities that detect when a security policy is being violated, many lack automated enforcement or prevention mechanisms. The second most prevalent attack vector in FY 2023 was "Email/Phishing," which represented the largest attack vector increase based on number of incidents (from 3,011 in FY 2022 to 6,198 in FY 2023).

Despite incident increases in certain categories of attack vectors, agencies have improved their ability to detect and categorize cyber attacks, which is evident in the significant decrease in incidents with "Other/Unknown" as the attack vector. The number of these uncategorized events has significantly dropped both in overall number of incidents (from 11,144 in FY 2022 to 5,687 in FY 2023) and the percentage of incidents when compared to the total for that year (from 38 percent in FY 2022 to 18 percent in FY 2023).

For the next fiscal year, per OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, CISA will continue to provide OMB with data regarding both individual agencies' performance in providing accurate, machine-readable data to CISA, as well as any gaps CISA has in receiving, updating, or maintaining such records. OMB and CISA continue to work with agencies to improve the quality of incident reporting data.

---

[11] NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide,* lists common vectors that are the method attack and provides expansive definitions of the attack vectors cited in this report. Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Table 3 Agency-Reported Incidents by Attack Vector

Attack Vector	FY22			FY23		
	CFO	Non-CFO	Total	CFO	Non-CFO	Total
Attrition An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	189	8	197	1,131	16	1,147
E-mail/Phishing An attack executed via an email message or attachment.	2,989	22	3,011	6,171	27	6,198
External/Removable Media An attack executed from removable media or a peripheral device.	46	1	47	92	0	92
Impersonation/Spoofing An attack involving replacement of legitimate content/services with a malicious substitute.	35	0	35	28	2	30
Improper Usage Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	10,280	210	10,490	11,923	338	12,261
Loss or Theft of Equipment The loss or theft of a computing device or media used by the organization.	1,748	84	1,832	3,052	83	3,135
Web An attack executed from a website or web-based application.	2,424	8	2,432	3,545	24	3,569
Other / Unknown An attack method does not fit into any other vector or cause of attack is unidentified.	10,928	216	11,144	5,441	246	5,687
Multiple Attack Vectors An attack that uses two or more of the above vectors in combination.	129	2	131	90	2	92
Total	28,768	551	29,319[12]	31,473	738	32,211

---

[12] FY 2022 figures reflect a correction to the incident counts and categories.

Incidents by NCISS Priority Level

Incidents reported to CISA are triaged and assigned a priority level calculated based on a variety of factors, including the level of impact.[13] The National Cyber Incident Scoring System (NCISS) provides a repeatable and consistent mechanism for estimating the risk of an incident across the Federal enterprise. Table 4 provides a high-level summary of incidents by NCISS priority level for FY 2022 and FY 2023.

The system is not intended to be an absolute scoring of the risk associated with an incident, but rather a relative mechanism for prioritization. It is not possible to conclude from this data whether there was a net increase or decrease in the risk level of reported incidents relative to the previous fiscal year. The vast majority of these incidents (accounting for approximately 97 percent in FY 2022 and 99 percent in FY 2023) were considered "baseline," meaning that per the Cybersecurity Incident Severity Schema, they are considered "unsubstantiated or inconsequential event[s]."

---

[13] The priority level could change as additional information is discovered during investigation.

Table 4 Agency-Reported Incidents[14] by NCISS Priority Level

NCISS Priority Level	FY22	FY23
Uncategorized *Insufficient information was collected in order to provide an NCISS priority level.*	263	229
Baseline – Negligible (White) *Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.*	16,449	14,086
Baseline – Minor (Blue) *Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	12,139	17,535
Low (Green) *Unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	491	348
Medium (Yellow) *May affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	1	31
High (Orange) *Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	0	0
Severe (Red) *Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.*	0	0
Emergency (Black) *Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.*	0	0
Total	**29,343**[15]	**32,229**

Major Incidents

Of the incidents reported by agencies in FY 2023, 11 were determined by agencies to meet the threshold for major incidents in accordance with the definition in M-23-03. The Departments of Health and Human Services, Justice, and Treasury reported multiple incidents.

Table 5 Summary of FY 2023 Major Incidents

Department of Health and Human Services
The United States Department of Health and Human Services (HHS) reported two major incidents in FY 2023. One involved a breach of Personally Identifiable Information (PII) caused by a ransomware attack against a contractor-owned and -operated system supporting HHS's Centers for Medicare and Medicaid

---

[14] Includes incidents report by entities outside of the Federal executive branch.
[15] FY 2022 figures reflect a correction to the incident counts and categories.

Services (CMS), specifically targeting network file shares. The exposed PII, which included beneficiary names, addresses, dates of birth, Medicare beneficiary identifiers, and bank account information, met the threshold to require mandatory major incident reporting (over 2.8 million individuals, over 1.3 million of which are deceased). The beneficiaries impacted have been notified and offered free credit monitoring services. Since the incident, Medicare beneficiary work has been moved from contractor networks to CMS networks.

HHS reported another major incident involving two contractor firms performing work for HHS. Attackers used a zero-day vulnerability to gain access to HHS program-related information hosted by the contractors, resulting in the potential compromise of PII. While there was no evidence of compromise to HHS networks and systems, the compromise to the contractor networks led to possible compromise of PII associated with the following operating divisions: Centers for Disease Control and Prevention, Administration for Community Living, Centers for Medicare and Medicaid Services, National Institutes of Health, and the Substance Abuse and Mental Health Services Administration. It is estimated that personal information on 1.88 million individuals may have been compromised—the information may include some combination of names, social security numbers, Medicare numbers, physical and email addresses, phone numbers, birth dates, gender, race, weight, height, medical diagnoses, and other individually identifiable or specific health-related information. HHS has taken required actions to notify individuals on a case-by-case basis.

Department of the Treasury
The United States Department of the Treasury (Treasury) reported two major incidents. One incident is a recurrence of a major incident from FY 2022. The Department of Treasury Internal Revenue Service (IRS) reported a major cybersecurity incident involving the inadvertent disclosure of 990-T forms (Exempt Organization Business Income Tax Return) filed by tax-exempt entities. The PII exposed was limited to names, addresses, e-mail addresses and phone numbers. The IRS is required to publicly disclose miscellaneous income earned by 501(c)3 organizations, which it does by publishing redacted copies of 990-T forms. To aid with this process, the IRS began using a vendor in September 2021 to assist with an automated process to publish these forms to a public facing website where subscribers could gain access. Due to a coding error, 990-T forms for all 501(c) entities were exposed until the error was disclosed to the agency by a private sector entity in early August of 2022. Once discovered, the IRS quickly notified subscribers and requested they delete the downloads. The IRS also worked with the vendor to fix the coding error. In their remediation efforts from the initial incident, the coding error was fixed on the public web server, however the erroneous data was not deleted from the staging server and the same data set was accidentally published a second time.

Treasury reported another major incident involving a phishing attack against an employee in their Office of the Inspector General (OIG). An advanced persistent threat (APT) nation state sponsored actor was able to obtain the employee's login credentials and gain access to the employee's account for approximately 15 hours. Due to defense in depth, the APT was unable to access any information resources during that time and no attempts were made to introduce malware or move laterally. The attacker was removed from the environment and steps were taken by Treasury to prevent recurrence such as awareness training, validating software configurations and updating multi-factor authentication policies.

Department of Justice

The United States Department of Justice (DOJ) reported two major incidents in fiscal year 2023. One of these incidents involved a ransomware attack in February 2023 on a United States Marshals Service's (USMS) computer system, containing Personally Identifiable Information (PII) from USMS personnel and legal processes. Upon discovery, the USMS immediately shut down the affected system and reconstituted the capabilities on a new USMS system to continue mission operations. Potentially impacted individuals, who were identified, have been notified, and offered free credit monitoring services.

DOJ reported another incident involving a ransomware attack in May 2023 against systems owned and operated by a private company providing case-specific data analytics support for the Civil Division and several United States Attorney's Offices. The company's system contained health records and other materials which included both PII and personal health information (PHI). The company hired a third-party incident response service provider to perform the incident investigation and response. Notification and offering of free credit monitoring services are in process for identified potentially impacted individuals.

Department of the Interior
The United States Department of the Interior (Interior) reported a major incident involving a system operated by the Interior Business Center (IBC). The system supports Interior and external Federal agency customers by providing Federal personnel and payroll services through interagency agreements. An authorized developer modified a security policy in this system that inadvertently allowed a limited number of human resources professionals to view personnel records of employees of 36 Federal agency customers. The investigation revealed that there were approximately 147,000 potentially affected individuals. The exposed PII included various combinations of subsets of records that contained employee name, address, email address, phone number, date of birth, place of birth, education, country of citizenship, and the last four digits of Social Security numbers. During the investigation, it was determined that a privacy impact assessment (PIA) was not conducted following recent changes to the system architecture—IBC has updated their security assessment and conducted an updated PIA. IBC provided notice to potentially affected individuals on behalf of the 36 Federal agencies and has strengthened change control procedures, internal processes, and training.

Consumer Financial Protection Bureau
The Consumer Financial Protection Bureau (CFPB) reported a major incident in response to a breach involving unauthorized transfer of CFPB records by a now-former employee to the employee's personal e-mail account. The employee sent 14 e-mails containing consumer PII and two spreadsheets with internal loan numbers of approximately 256,000 consumers of a single financial institution. As part of the breach remediation and mitigation efforts, CFPB provided instructions to the now-former employee to delete the e-mails from their personal account, certify each e-mail was deleted, and provide attestation once those actions were completed. The former employee did not comply with the efforts. CFPB also notified and conferred with the institution impacted by the breach. Though the impacted PII did not include sensitive information that can be used to access a consumer's account or commit identity theft, CFPB determined in some cases that notifying consumers was appropriate in an abundance of caution and as a matter of transparency. Additionally, CFPB referred this matter to the Office of the Inspector General for further investigation.

CFPB initiated and executed additional operational and technical mitigation efforts to strengthen the cybersecurity and privacy posture and prevent inadvertent breaches from occurring in the future.

Internal communications and training have been conducted with all CFPB employees and contractors informing them of the major incident, reiterating to all staff their responsibilities to comply with cybersecurity and privacy policies, and reinforcing to the workforce the importance and responsibility of maintaining proper storage and transmission of CFPB data. Additionally, CFPB conducted an internal review of the information management procedures and processes related to their supervision program to identify areas for improvement and opportunities to further improve privacy or security controls.

Department of Transportation

The United States Department of Transportation (DOT) reported a major cyber incident involving the compromise of several administrative systems and confirmed evidence of system access and exfiltration of PII from the Parking and Transit Benefit System (PTBS) which is the information system that supports TRANServe. Unknown attackers gained access by leveraging an unpatched critical vulnerability in a commercial web-application development platform. Potentially affected individuals numbered 237,000 and included in the PII were user names, home and work address, and the last four digits of social security numbers from some agencies. Affected servers have been rebuilt on new platforms using the latest patch. Potentially affected individuals were notified and offered free credit monitoring services.

Office of Personnel Management

The United States Office of Personnel Management (OPM) reported a major incident involving an unknown (zero-day) critical vulnerability in a file transfer software product used by a contractor responsible for supporting the administration of the Federal Employee Viewpoint Survey (FEVS). OPM was notified of this major incident by the contractor. The information compromised consisted of a listing of individuals' Government e-mail addresses, FEVS survey links (unique to each individual), and OPM's internally-generated tracking codes for approximately 632,000 employees within the United States Department of Justice and the United States Department of Defense (DoD).

In response, OPM halted the transfer of any FEVS data or records to the contractor using that software product, deactivated individual-specific survey links, conducted harm assessment and notified potentially affected individuals. The harm assessment found there was no evidence of unauthorized access or manipulation of survey results.

Department of Energy

The United States Department of Energy (DOE) reported a major incident involving a zero-day vulnerability with a secure file transfer product affecting DOE's Waste Isolation Pilot Plant (WIPP) and the Oak Ridge Associated Universities (ORAU). The vulnerability allowed for a known ransomware group to exploit the vulnerability allowing for remote access. The group claimed to have removed data from Government networks and in response DOE declared a major incident. Exposed information included PII and PHI on 34,000 individuals covered by a Congressionally mandated voluntary health monitoring program under a cooperative agreement with the Office of Environment, Health, Safety, and Security (EHSS) for former DOE employees who may have been exposed to dangerous substances such as nuclear waste. The information included names, dates of birth, social security numbers, and some health information. Approximately 66,000 individuals from the Office of Science were also affected—PII included names, dates of birth, partial or full social security numbers, passport information, and nationalities. Impacted individuals were notified and provided identity monitoring services.

Section III: Senior Agency Official for Privacy (SAOP) Performance Measures

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of (collectively, "handles") personally identifiable information (PII)[16] to carry out its missions and programs. In today's digital world, effectively managing the risk to individuals associated with the Federal Government's processing of their PII depends on Federal agencies maintaining robust privacy programs.

This section reflects reporting to OMB by 24 CFO Act agencies and 65 non-CFO Act agencies on FY 2023 SAOP FISMA performance measures.[17]

A. Senior Agency Officials for Privacy (SAOPs) and Privacy Programs

Executive Order 13800 recognizes that effective risk management requires the heads of Federal agencies to lead integrated teams of senior executives, including executives with expertise in privacy. While the head of each Federal agency remains ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within that agency, Executive Order 13719, *Establishment of the Federal Privacy Council*, requires the heads of agencies to designate or re-designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for the agency's privacy program.

Each Federal agency is required to develop, implement, document, maintain, and oversee an agency-wide privacy program that includes people, processes, and technologies. The agency's SAOP leads the agency's privacy program and is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission. Among other things, where PII is involved, the agency's privacy program plays a key role in information security, records management, strategic planning, budget and acquisition, contractors and third parties, workforce, training, incident response, and implementation of the NIST Risk Management Framework (RMF).[18]

---

[16] The term "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. *See* OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) [hereinafter "OMB Circular A-130"], § 10(a)(57).

[17] A total of 66 non-CFO Act agencies submitted SAOP FISMA performance measures for FY 2023. Among the submissions from those agencies, 65 agencies' responses were sufficiently complete to yield meaningful summary data.

[18] *See* OMB Circular A-130 at Appendix II § 5.

Table 6 Senior Agency Officials for Privacy (SAOPs) and Privacy Programs

FY 2023 – SAOP FISMA Performance Measures[19]	CFO	Non-CFO
The head of the agency has designated an SAOP.[20]	100%	100%
Among the agencies that have designated an SAOP:		
The SAOP has the necessary role and responsibilities within the agency for compliance.[21]	100%	97%
The SAOP has the necessary role and responsibilities within the agency for policy making.[22]	100%	97%
The SAOP has the necessary role and responsibilities within the agency for risk management activities.[23]	100%	97%
The agency has developed and maintained a privacy program plan.[24]	100%	89%
Among the agencies that have developed and maintained privacy program plans, the agency's privacy program plan includes a description of resources dedicated to the privacy program.[25]	100%	97%

B. Personally Identifiable Information and Social Security Numbers

Federal agencies' privacy programs are required to maintain an inventory of information systems that process PII. Maintaining such an inventory allows privacy programs to have an ongoing awareness of their PII holdings and helps to ensure compliance with applicable privacy requirements and to manage privacy risks.

---

[19] Percentages are rounded to the nearest whole number throughout the SAOP performance measures.

[20] *See* OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).

[21] *See id.*

[22] *See id.*

[23] *See id.*

[24] Federal agencies are required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the privacy program structure, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. *See* OMB Circular A-130 at Appendix I § 4(c)(2), 4(e)(1).

[25] *See id.* at Appendix I § 4(b)(1).

Table 7 Personally Identifiable Information Inventory

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains an inventory of the agency's information systems[26] that handle PII.[27]	100%	97%

In addition to ensuring compliance and managing the privacy risks associated with PII generally, Federal agencies are required to take additional steps to manage the risk associated with the collection, maintenance, and use of Social Security numbers (SSNs). Historically, the Federal Government has collected SSNs in many contexts, including employment, taxation, law enforcement, and benefits administration. However, SSNs are also key pieces of identifying information that could potentially be used to perpetrate identity theft. Therefore, per OMB Circular A-130, Federal agencies are required to take steps to eliminate the unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as a personal identifier.

Table 8 Collection, Maintenance, and Use of Social Security Numbers (SSNs)

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that collect, maintain, or use SSNs, the agency has an inventory of the agency's collection and use of SSNs.[28]	100%	89%
Among the agencies that collect, maintain, or use SSNs; have inventories of their collection, maintenance, and use of SSNs; and maintain inventories of information systems, the agency maintains the inventory of SSNs as part of the agency's inventory of information systems that handle PII.	100%	93%
The agency has developed and implemented a written policy to help ensure that any new collection or use of SSNs is necessary.	96%	78%
Among the agencies with such written policies:		

---

[26] The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *See* 44 U.S.C. § 3502(8). The term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology. *See* 44 U.S.C. § 3502(6). The term "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. *See* OMB Circular A-130 at § 10(a)(23).

[27] *See* OMB Circular A-130 at § 5(a)(1)(a)(ii), 5(f)(1)(e).

[28] Federal agencies are not required to have an inventory of collection and use of SSNs. However, agencies need to have a sufficient evidentiary basis to determine whether they have met the requirement to eliminate unnecessary collection and use of SSNs.

	CFO	Non-CFO
The agency's written policy provides specific criteria to use when determining whether the collection or use of SSNs is necessary.	100%	90%
The agency's written policy establishes a process to ensure that any collection or use of SSNs determined to be necessary remains necessary over time.	96%	94%
Among the agencies that collect, maintain, or use SSNs and have not already eliminated all unnecessary collection, maintenance, and use of SSNs by the agency, the agency has taken steps during the reporting period to eliminate the unnecessary collection, maintenance, and use of SSNs.[29]	96%	90%

C. Privacy and the Risk Management Framework

In order to effectively manage the risk to individuals associated with the processing of their PII, Federal privacy programs have specific responsibilities under the NIST RMF. The NIST RMF is a disciplined and structured process that Federal agencies use to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of information security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.

Table 9 Privacy and the NIST Risk Management Framework

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that have implemented a risk management framework, that framework guides and informs:		
Categorization of Federal information and information systems that process PII.[30]	96%	98%
Selection, implementation, and assessment of privacy controls.[31]	96%	93%
Authorization of information systems and common controls.[32]	100%	93%
Continuous monitoring of information systems that process PII.[33]	96%	85%
The agency has designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls.[34]	100%	75%

---

[29] *See* OMB Circular A-130 at § 5(f)(1)(f).
[30] *See* OMB Circular A-130 at Appendix I § 3(a), 3(b)(5).
[31] *See id.*
[32] *See id.*
[33] *See id.*
[34] *See id.* at Appendix I § 4(e)(5); *see also id.* at § 10(a)(14), (26), (66) and (86).

The agency has developed and maintained a written privacy continuous monitoring strategy.[35]	88%	78%
The agency has established and maintained an agency-wide privacy continuous monitoring program.[36]	88%	69%

Agencies are required to authorize information systems prior to operation and periodically thereafter. Authorization of an information system is an explicit acceptance of the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of the security and privacy controls. The determination to authorize the information system is based on a review of the information system authorization package, which includes the security plan, the privacy plan, documented assessments of the security and privacy controls, and any relevant plans of action and milestones. In accordance with OMB Circular A-130, when an information system processes PII, the determination to authorize the information system is made in coordination with the SAOP.

Table 10 Information Systems and Authorizations to Operate

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period.[37]	3,942	635
Information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period where the SAOP reviewed and approved the categorization of the information system.[38]	92%	87%

---

[35] The SAOP is required to develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. *See* OMB Circular A-130 at Appendix I § 4(d)(9), 4(e)(2).

[36] The SAOP is required to establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. *See* OMB Circular A-130 at Appendix I § 4(d)(10)-(11), 4(e)(3).

[37] Federal agencies are required to provide oversight of information systems used or operated by contractors and other entities on behalf of the Federal Government, including ensuring that these information systems are included in their respective inventory of information systems. *See* OMB Circular A-130 at Appendix I § 4(j)(2)(c).

[38] *See id*. at Appendix I § 4(a)(2), 4(e)(7).

	CFO	Non-CFO
Information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period where the SAOP reviewed and approved a system privacy plan for the information system prior to the information system's authorization or reauthorization.[39]	88%	82%
Information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period where the SAOP conducted and documented the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented for the information system prior to the information system's authorization or reauthorization.[40]	89%	77%
Information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period where the SAOP reviewed the information system's authorization package to ensure compliance with applicable privacy requirements and manage privacy risks, prior to the authorizing official making a risk determination and acceptance decision.[41]	88%	88%

D. Information Technology Systems and Investment

Effectively managing the risk to individuals associated with the processing of their PII requires that Federal privacy programs consider the potential impact on individuals' privacy throughout the system development lifecycle. Federal agencies are required to consider privacy when analyzing IT investments, and are required to establish a decision-making process that covers the lifecycle of each information system. That includes creating explicit criteria for analyzing the projected and actual costs, benefits, and risks, including privacy risks, associated with any IT investments.

Table 11 Information Technology Systems and Investments

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has a policy that includes explicit criteria for analyzing privacy risks when considering IT investments.[42]	83%	69%

---

[39] Federal agencies are required to develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. *See* OMB Circular A-130 at Appendix I § 4(c)(9), (e)(8).

[40] *See id*. at Appendix I § 4(e)(3).

[41] *See id*. at Appendix I § 4(e)(9).

[42] *See id*. at § 5(d)(3).

The agency reviewed IT capital investment plans and budgetary requests during the reporting period to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, were explicitly identified and included, with respect to any IT resources that will be used to handle PII.[43]	83%	77%
The agency maintains an inventory of the agency's information technology systems that handle PII.	100%	98%

E. Privacy Impact Assessments

Privacy impact assessments (PIAs) are one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks when developing, procuring, or using IT. As a general matter, Federal agencies are required to conduct PIAs, absent an applicable exception, when they develop, procure, or use IT to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. SAOPs work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials in order to conduct a meaningful assessment.

Table 12 Privacy Impact Assessments

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a PIA under the E-Government Act of 2002.	4,913	904
IT systems maintained, operated, or used by an agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a PIA under the E-Government Act of 2002 that are covered by an up-to-date PIA.[44]	81%	83%

---

[43] *See id.* at § 5(a)(3)(e)(ii).

[44] Federal agencies are required to update PIAs whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology. For the purposes of this question, an up-to-date PIA is a PIA that reflects any changes to the information technology, changes to the agency's practices, or other factors that alter the privacy risks associated with the use of such information technology. *See* OMB Circular A-130 at Appendix II § 5(e).

Among the agencies that have a written policy for PIAs, the written policy for PIAs includes:[45]		
A requirement for PIAs to be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA.	100%	94%
A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs.	100%	96%
A requirement for PIAs to be updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks associated with the use of a particular IT system.	100%	98%
The agency has a process or procedure for:[46]		
Assessing the quality and thoroughness of each PIA.	100%	80%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	100%	83%
Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated.	100%	80%
Ensuring that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks.	100%	80%

F. Workforce Management

Federal agencies' privacy programs are required to play a key role in workforce management activities and in holding agency personnel accountable for complying with applicable privacy requirements and managing privacy risks. This includes developing, maintaining, and providing agency-wide privacy awareness and training programs for all employees and contractors. In addition, the SAOP is required to be involved in assessing the hiring and professional development needs with respect to privacy at their agency.

Table 13 Workforce Management

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency ensures that the agency's privacy workforce has the appropriate knowledge and skill.[47]	88%	100%

---

[45] *See id.* at Appendix II § 5(e) (July 28, 2016).
[46] *See* OMB Circular A-130 at Appendix II § 5(e).
[47] *See* OMB Circular A-130 at § 5(c)(2).

The agency has assessed its hiring, training, and professional development needs with respect to privacy during the reporting period.[48]	100%	92%
The agency has developed a workforce planning process to ensure that it accounts for privacy workforce needs.[49]	79%	74%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions.[50]	79%	83%

Table 14 Training and Accountability

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency provides foundational privacy training to its Federal employees (including managers and senior executives).[51]	100%	95%
The agency provides role-based privacy training to its Federal employees with assigned privacy roles and responsibilities, including managers, before authorizing their access to Federal information or information systems.[52]	83%	66%
The agency has ensured that measures are in place to test the knowledge level of information system users in conjunction with privacy training.[53]	96%	78%
The agency has established rules of behavior, including consequences for violating rules of behavior, for Federal employees that have access to Federal information or information systems, including those that handle PII.[54]	100%	98%
Among the agencies that have established rules of behavior, the agency ensures that Federal employees have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.[55]	100%	100%

---

[48] *See id.* at § 5(c)(6).
[49] *See id.* at § 5(c)(1).
[50] *See id.*
[51] *See id.* at Appendix I § 4(h)(4); *see also id.* at Appendix I § 4(h)(1).
[52] *See id.* at Appendix I § 4(h)(5); *see also id.* at Appendix I § 4(h)(1).
[53] *See id.* at Appendix I § 4(h)(4).
[54] *See id.* at Appendix I § 4(h)(6).
[55] *See id.* at Appendix I § 4(h)(7).

Table 15 Contractors and Third Parties

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors.[56]	100%	86%
The agency has established rules of behavior, including consequences for violating rules of behavior, for contractors that have access to Federal information or information systems, including those that handle PII.[57]	100%	97%
Among the agencies that have established rules of behavior, the agency ensures that contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.[58]	100%	97%
The extent to which the agency ensures that terms and conditions in contracts and other agreements involving the handling of Federal information incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information:[59]		
Processes do not exist.	0%	0%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	17%	26%
Processes are fully documented and implemented and cover all relevant aspects.	4%	18%
Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current.	79%	55%
The extent to which the agency ensures appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information:[60]		
Processes do not exist.	0%	0%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	0%	23%

---

[56] *See id.* at Appendix I § 4(h)(1), (4)-(5).
[57] *See id.* at Appendix I § 4(h)(6).
[58] *See id.* at Appendix I § 4(h)(7).
[59] *See id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).
[60] *See id.* at Appendix I § 4(j)(2)(a).

Processes are fully documented and implemented and cover all relevant aspects.	17%	18%
Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current.	83%	58%

G. Breach Response and Privacy

Federal agencies' privacy programs and their respective SAOPs are required to include specific steps to prepare for and respond to a breach (i.e., an incident that involves PII). This includes developing and implementing a breach response plan that describes, among other things, the composition of the agency's breach response team, the factors the agency shall consider when assessing the risk of harm to potentially affected individuals, and if, when, and how to provide notification to potentially affected individuals and reporting to other relevant entities.[61]

Table 16 Breach Response

FY 2023 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that have a breach response plan, the breach response plan includes the agency's policies and procedures for:[62]		
Reporting a breach	100%	100%
Investigating a breach	100%	100%
Managing a breach	100%	100%
Among the agencies that have a breach response plan, the SAOP reviewed the agency's breach response plan during the reporting period to ensure that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology.[63]	100%	90%
The agency has a breach response team composed of agency officials designated by the head of the agency that can be convened to lead the agency's response to a breach.[64]	96%	97%

---

[61] *See* OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).
[62] *See id.* at § VII, XI.
[63] *See id.* at § X.B, XI.
[64] *See id.* at § VII.A, XI.

Among the agencies with a breach response team, the agency's breach response team participated in at least one tabletop exercise during the reporting period.[65]	83%	63%
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that were reported within agencies during the reporting period.[66]	18,909	791
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that agencies reported to the DHS Cybersecurity and Infrastructure Security Agency (CISA) during the reporting period.[67]	8,420	167

---

[65] *See id.* at § X.A, XI.
[66] *See id.* at § III.C, XI.
[67] *See id.* at § VII.D.1, XI.

Appendix I: Agency Cybersecurity Performance Summaries

This report promotes transparency and enhances accessibility to information on the unique missions, resources, and challenges of each agency by providing agency-specific narratives entitled "Cybersecurity Performance Summaries," which can be found here. Each summary contains four sections: CIO Rating, CIO Self-Assessment, Independent Assessment, and a count of incidents reported by attack vector. The descriptions below provide an overview of the sections included in each agency performance summary.

Independent Assessments and IG Ratings

This independent narrative section requests independent assessors (most often agency IGs) to frame the scope of their analysis, identify key findings, and provide high level recommendations to address those findings.

Independent assessors evaluate each agency's information security program and provide ratings for each of the NIST CSF functions based on a five-level maturity model, as described in FY 2023-2024 Inspector General FISMA Reporting Metrics:

- *Ad-hoc* (Level 1): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
- *Defined* (Level 2): Policies, procedures, and strategies are formalized and documented but not consistently implemented.
- *Consistently Implemented* (Level 3): Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- *Managed and Measurable (Level 4):* Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
- *Optimized (Level 5):* Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs

Appendix II: Commonly Used Acronyms

APMD: *Anti-Phishing and Malware Defense*
ATO: *Authority to Operate*
BOD: *Binding Operational Directive*
CAP Goals: *Cross-Agency Priority Goals*
CDM: *Continuous Diagnostics and Mitigation Program*
CDOC: *Chief Data Officers Council*
CEO: *Chief Executive Officer*
CFO: *Chief Financial Officer*
CIGIE: *Council of the Inspectors General on Integrity and Efficiency*
CIO: *Chief Information Officer*
CIOC: *Chief Information Officer Council*
CISA: *Cybersecurity and Infrastructure Security Agency*
CISO: *Chief Information Security Officer*
CISOC: *Chief Information Security Officer Council*
CSF: *Cybersecurity Framework*
CSP: *Cloud Service Provider*
CVD: *Coordinated Vulnerability Disclosure*
DLP: *Data Loss Prevention*
DHS: *Department of Homeland Security*
ED: *Emergency Directive*
EOP: *Executive Office of the President*
ERM: *Enterprise Risk Management*
FAI: *Federal Acquisition Institute*
FBI: *Federal Bureau of Investigations*
FCEB: *Federal Civilian Executive Branch*
FedRAMP: *Federal Risk and Authorization Management Program*
FIPS: *Federal Information Processing Standards*
FPC: *Federal Privacy Council*
FY: *Fiscal Year*
GFE: *Government Furnished Equipment*
GSA: *General Services Administration*
HVA: *High Value Asset*
HWAM: *Hardware Assets Management*
IC: *Intelligence Community*
ICAM: *Identity, Credential, and Access Management*
IG: *Inspector General*
ISCM: *Information Security Continuous Monitoring*

NCCIC: *National Cybersecurity and Communications Integration Center*
NCISS: *National Cyber Incident Scoring System*
NCPS: *National Cybersecurity Protection System*
NIST: *National Institute of Science and Technology*
NSA: *National Security Agency*
NSCC: *National Security Coordination Council*
NSS: *National Security System*
ODNI: *Office of the Director of National Intelligence*
OFCIO: *Office of the Chief Information Officer*
OIG: *Office of the Inspector General*
OIRA: *Office of Information and Regulatory Affairs*
OMB: *Office of Management and Budget*
ONCD: *Office of the National Cyber Director*
PAM: *Privileged Access Management Tool*
PIA: *Privacy Impact Assessment*
PII: *Personally Identifiable Information*
PIV: *Personal Identity Verification*
POA&M: *Plan of Actions and Milestones*
RMA: *Risk Management Assessment*
RMF: *Risk Management Framework*
RVA: *Risk and Vulnerability Assessment*
SAOP: *Senior Agency Official for Privacy*
SAR: *System Architecture Review*
SCAP: *Security Content Automation Protocol*
SCRM: *Supply Chain Risk Management*
SECURE Technology Act: *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*
SMTP: *Simple Mail Transfer Protocol*
SP: *Special Publication*
SSL: *Secure Sockets Layer*
SSN: *Social Security Number*
SWAM: *Software Asset Management*
TIC: *Trusted Internet Connection*
TLS: *Transport Layer Security*
US-CERT: *United States Computer Emergency Readiness Team*
VDP: *Vulnerability Disclosure Policy*
VPN: *Virtual Private Network*