FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

ANNUAL REPORT FISCAL YEAR 2022

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 2022 data reported by agencies to OMB and DHS.

Table of Contents

Executive Summary: The State of Federal Cybersecurity

As stated in President Biden's Executive Order on Improving the Nation's Cybersecurity (EO 14028), "the United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." In Fiscal Year (FY) 2022, the Administration took actions to continue implementation of EO 14028, including migration to a zero trust architecture and alignment of Federal agency investments in cybersecurity defenses with policy requirements. With these actions, the Federal Government seeks to rapidly shift to a new cybersecurity paradigm and dramatically reduce the risk of successful cyber attacks against our digital infrastructure.

The Federal Chief Information Security Officer was designated to serve as the first Deputy National Cyber Director for Federal Cybersecurity in October 2021, as part of the Administration's ongoing effort to ensure a cohesive and coherent Federal approach to cybersecurity. This "dual hat" arrangement ensures that the Administration speaks with one voice when it comes to the defense of the Federal Government's digital infrastructure and prioritizes resources in a collaborative manner.

The cybersecurity priority for the Office of Management and Budget (OMB) and Federal agencies in FY 2022 was to continue implementation of EO 14028. This report highlights the actions and progress achieved since EO 14028 was issued. In FY 2022, OMB issued five memoranda to improve the Federal Government's ability to detect, identify, deter, protect against, and respond to modern threats and threat actors. In January 2022, OMB released OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09), also known as the Federal Zero Trust Strategy, to direct agencies to invest in technology that is built and deployed with security foremost in mind and move towards a zero trust architecture that provides the vigilance needed to detect malicious behaviors and react quickly.

The Federal Zero Trust Strategy requires agencies to achieve specific zero trust security goals by the end of FY 2024. These goals align with the Cybersecurity and Infrastructure Security Agency's (CISA) five zero trust pillars: Identity; Devices; Networks; Applications and Workloads; and Data. M-22-09 requires agencies to adopt leading security practices, such as phishing-resistant multi-factor authentication (MFA); to implement industry best practices for encryption; and to ensure device-level signals are used in determining access to Federal systems. In addition to these defensive measures, OMB initiated a Federal Government-wide shift towards the use of software developed in a secure manner by issuing OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Development Practices* (M-22-18). This memorandum ensures that the software used by agencies is developed in a secure manner, minimizing or eliminating the risks associated with running unvetted technologies on agency networks, and increasing the resilience of Federal technology in the face of cyber threats.

To ensure Federal agencies are prioritizing efforts and resources to achieve the goals laid out in EO 14028 and subsequent OMB memoranda, OMB and the Office of the National Cyber Director (ONCD)

jointly issued *Administration Cybersecurity Priorities for the FY 2024 Budget* (M-22-16). This document outlines the Administration's cyber investment priorities, providing guidance to agencies regarding areas of emphasis for formulating their FY 2024 proposals.

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

FY22 Report Key Takeaways:

30,659 incidents were reported in FY 2022.

This is a 5.7 percent decrease from FY 2021. Three were reported as major incidents.[1]

Agencies show improvements in adoption of cyber defensive measures.

However, more work is necessary and agencies must continue to drive adoption of zero trust priorities such as phishing resistant multi-factor authentication.

Agencies are well positioned to respond to incidents, should they occur.

Every agency worked to evaluate CISA's Cybersecurity Incident and Vulnerability Response Playbooks against their current incident response procedures and determined a process for sharing incident details electronically with CISA.

[1] While the trend is encouraging, drawing conclusions based on this data point, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years, would be premature. Major incidents were reported in accordance with the definition of that term established in M-22-05.

Section I: Federal Cybersecurity Activities

A. Implementing a Zero Trust Architecture

Executive Order 14028 (EO 14028)

President Biden issued EO 14028 to take bold action towards modernizing Federal cybersecurity defenses by protecting Federal systems, improving information-sharing between the Federal Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur.

This is especially important as FY 2022 marked a paradigm shift in how the Federal Government approaches cybersecurity. To implement EO 14028 and subsequent policies, OMB and other agencies focused on making Federal systems more defensible by employing zero trust principles premised on the idea that trust is never granted implicitly but must be continually evaluated. As President Biden stated in EO 14028, "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

OMB issued three memoranda in FY 2022 that will accelerate zero trust adoption and bolster cyber defenses across the Federal Government:

- M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (October 8, 2021);
- M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022); and
- M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (September 14, 2022).

In collaboration with OMB, CISA's CyberStat program hosted six workshops focused on zero trust implementation. CyberStat workshops are designed to provide agencies with the necessary support, guidance, and access to resources to assist them in implementing the actions contained in the EO and OMB Circulars and Memoranda.

Throughout FY 2022, OMB tracked agencies' progress toward zero trust goals through CIO FISMA metrics which reflect a dramatic change in the way success is measured from previous years. In FY 2022, agencies were asked to submit new data that corresponded to newly issued policies. The shift in metrics reflect the systemic change the Administration is seeking in shifting to a zero trust architecture. They include adoption rates for both phishing-resistant and non-phishing resistant MFA and logging; incorporation of security measures for critical software; and patching prioritization. Reporting on these new CIO FISMA metrics enabled agencies to further align to the vision outlined in EO 14028 and allowed OMB and other security stakeholders to share insights on areas of success and those that need further investment. Notably, every agency reported the use of a patch management process that prioritized patching based on the severity of a vulnerability. This action enables agency

security personnel to focus limited resources on the most critical vulnerabilities, which helps protect the agency as it continues to deliver on its mission.

After assessing FY 2022 data, OMB published the Federal Cybersecurity Progress Report to provide the public with a precise, fair, and comprehensive assessment of agency cybersecurity posture. OMB will continue overseeing agencies' implementation of Administration cybersecurity policies through CIO FISMA metrics.

B. Program and Policy Areas

Federal Zero Trust Strategy

The Federal Zero Trust Strategy (M-22-09) is an outcome-focused policy centered on five pillars: Identity; Devices; Networks; Applications and Workloads; and Data. M-22-09 directs agencies to take specific zero trust actions by defined deadlines, with full implementation to be completed by the end of FY 2024. These actions include submitting an agency-specific zero trust implementation plan to OMB and CISA, identifying a zero trust implementation lead for each agency, providing a phishing-resistant option to public users for public-facing agency systems that support MFA, and removing password policies that require special characters and regular rotation, among several other items.

All 24 Chief Financial Officers (CFO) Act agencies and 46 non-CFO Act agencies submitted zero trust implementation plans, which were reviewed by OMB and CISA. OMB and CISA held sessions with these agencies to discuss their plans, a significant first step to advancing the vision of EO 14028 and implementation of M-22-09 guidance. Agency zero trust implementation plans show that they have assessed their environments, understand the resources required to implement their zero trust plans, and are progressing toward alignment of resources to address cyber risks.

In addition to developing and executing on a plan for zero trust, agencies are collaborating with one another to accelerate key actions outlined in the Federal Zero Trust Strategy. In FY 2022, OMB established the Identity Credentialing and Access Management Community of Action (CoA) focused on the deployment of industry-leading technical capabilities for authentication. OMB intends to establish additional CoAs in FY 2023.

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 civilian 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, Logical Response Aperture; Intrusion Prevention; Analytics; Information Sharing; and Core Infrastructure. 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 2022, CISA and OMB identified CIO FISMA metrics that could be reported in an automated manner. Automation will be increasingly used to reduce the reporting burden on agencies and improve the insight into agency security provided by the FY 2023 CIO FISMA Metrics.

Through funding made available from the American Rescue Plan Act (ARPA) in FY 2021, CISA began acquiring Endpoint Detection and Response (EDR) tools for 50 agencies, including both CFO Act agencies (10 agencies) and non-CFO Act agencies (40 agencies). As of the end of FY 2022, there are 48 agencies that either use EDR solutions deployed by CISA or have self-attested to achieving greater than 80 percent coverage of known endpoints. During FY 2022, the CDM program made significant progress in making available and deploying enterprise EDR and mobile security solutions in support of EO 14028 by:

- Achieving active deployment with 12 CFO Act agencies and over 20 non-CFO Act agencies, several of which have met the necessary criteria for EDR to be considered fully deployed there;
- Offering CISA support to all Federal agencies and meeting the needs of all agencies that have expressed a need;
- Initiating the first phase of Host Level Visibility (HLV) rollouts;
- Completing Enterprise Mobility Management (EMM) integration at one CFO Act agency;
- Achieving development or deployment status with 6 additional CFO Act agencies; and
- Completing EMM designs for non-CFO Act agencies, with deployments that began in September 2022.

Additionally, the CDM Program has supported identity management deployments at 11 CFO Act agencies and 2 non-CFO Act agencies and modernized the CDM Dashboard capability to support visibility improvements under our Memorandum of Agreement 2.0. In FY 2023, the CDM program will work with agencies to continue EDR deployments and begin rollout of Mobile Threat Defense (MTD).

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), Logical Response Aperture; Intrusion Prevention (EINSTEIN 3 Accelerated (E3A)); Analytics; Information Sharing; and Core Infrastructure.

In FY 2022, DHS CISA began efforts to rescope the NCPS and establish a new program – the Cyber Analytic and Data System (CADS), a system of systems that provides a robust and scalable analytic environment capable of integrating data sets while also providing tools and capabilities. CADS is being established to provide the mission infrastructure, analytic tools, and engineering expertise to integrate formerly stove-piped data sets, provide 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 Federal agencies; 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 2022 focused on expanding the analytic environment (AE) infrastructure to support additional datasets, developing a data integration roadmap, initiating migration of on-premises capabilities to the cloud AE, and implementing additional analytic tools in the cloud AE. CISA has made considerable progress towards these transition goals; 74 percent of tools were migrated as of FY 2022 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 ingested into the CADS AE to allow our Federal Government cyber defenders to automate certain protections, as well as quickly detect and halt nefarious activity before it can move laterally into sensitive Federal systems. This transition is part of a recognition that every device that connects to a Federal system is a potential attack vector for cyber threats.

Intrusion Prevention and Intrusion Detection services (otherwise referred to as the EINSTEIN sensor suite) are not in scope of the CADS program. Intrusion Prevention services provided through EINSTEIN 3 Accelerated (E3A) will end in FY 2024. With the initial implementation of a new Protective DNS service, the number of agencies using E3A has decreased from 87 to 79. The FY 2023 FISMA report will provide updates on these transitions as appropriate.

Table 1 demonstrates NCPS implementation status as of September 30, 2022. Future iterations of this report may include updates on the transition to CADS as outlined above.

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

		Complete		In Progress		Deferred[1]		Not Implemented	
		FY21	FY22	FY21	FY22	FY21	FY22	FY21	FY22
Einstein Capability	**E1/E2**	**82**	**85**	**1**	**1**	**0**	**0**	**21**	**18**
	CFO	23	23	0	0	0	0	0	0
	Non-CFO	59	62	1	1	0	0	21	18
	E3A Email	**82**	**85**	**3**	**0**	**5**	**5**	**14**	**14**
	CFO	23	23	0	0	0	0	0	0
	Non-CFO	59	62	3	0	5	5	14	14
	E3A DNS	**87**	**79**	**1**	**0**	**3**	**0**	**13**	**15**
	CFO	23	19	0	0	0	0	0	0
	Non-CFO	64	60	1	0	3	0	13	15
	Protective DNS	**0**	**10**						
	CFO	0	4						
	Non-CFO	0	6						

Vulnerability Disclosure Policies

Vulnerability disclosure policies (VDP) enable agencies to improve their information security programs by welcoming cybersecurity review from external researchers. VDPs enable agencies to obtain new insights into security vulnerabilities and understanding of the agency's external risk posture, which provides high return on investment. VDPs also provide protection for those who uncover these vulnerabilities by explicitly authorizing good-faith security research. In FY 2021, agencies published their VDPs on their primary .gov websites and developed implementation plans which provided timelines and milestones for those policies. In FY 2022, all CFO Act agencies other than the

Department of Defense[2] reported the establishment of a VDP, with over 80 percent of agencies reporting the establishment of a VDP that covered either internet accessible systems or all 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 and to better enable the identification and risk assessment of the overall Federal HVA enterprise. HVA Assessments collaboratively evaluate the risk management posture of a High Value Asset.

Agencies may designate Federal information or a Federal information system as an HVA when it falls into one or more of the following categories:[3]

- *Informational Value* – The information or the 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 the 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 maintenance of an unbiased view of the risk associated with maintaining an HVA. Agencies are therefore required to ensure HVA assessments are conducted in accordance with CISA requirements.[4]

[2] 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 is not included in this analysis.

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

[4] M-19-03 and CISA Binding Operational Directive 18-02.

In FY 2022, assessments of HVA systems continued to identify challenges 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.

Figure 1 Top 5 High Value Asset Assessment Findings in FY22

1	**Patch Management**
2	**Unsupported OS or Application**
3	**Authentication Bypass**
4	**Database Configuration**
5	**Insecure Default Configuration**

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 and Risk and Vulnerability Assessments—each requiring individual visits. To address this issue and to avoid backlogs, CISA's HVA Program Management Office revised the assessment process by combining the SAR and RVA into a single methodology. Using this new approach for the first time in FY 2021, CISA conducted 46 total HVA assessments, resulting in 263 findings. During FY 2022, a total of 48 assessments were conducted, with 433 findings. Put another way, in FY 2021 there were 5.7 findings per visit, and in FY 2022, there were nine per visit. Patch management, which was the top finding in FY 2021, remained the number one finding in FY 2022. Unsupported OS or application appeared for the first time as a finding in five years (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 was not a finding in FY 2021, but issues related to authentication (e.g., weak passwords, admin password re-use) appeared as findings in previous fiscal years 2017-2020 and remain a significant concern. Database Configuration and Insecure Default Configuration remained the fourth and fifth most typically identified findings for FY 2022—the same ranking as FY 2021.

Trusted Internet Connections

In October 2021, CISA updated the Trusted Internet Connections (TIC) 3.0 Remote User Use Case and the Security Capabilities Catalog based on the policy in OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*.

In June 2022, CISA released a draft version of the TIC Cloud Use Case, which addresses cloud deployments of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Email-as-a-Service (EaaS), and an updated Security Capabilities catalog with 38 new capabilities. CISA conducted a Request for Comments (RFC) period that closed in July 2022 and updated both documents based on the comments received.

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 certain 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 one BOD and two EDs in FY 2022:

- **BOD 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities**: On November 3, 2021, BOD 22-01 required agencies to review and update internal vulnerability management policies and procedures to include BOD-specified minimum requirements. Agencies were further required to remediate each vulnerability according to timelines set forth in the CISA-managed vulnerability catalog and report on the status of vulnerabilities listed in the repository.
- **ED 22-02 – Mitigate Apache Log4J Vulnerability (Closed)**: On December 17, 2021, ED 22-02 was issued following the discovery of a series of vulnerabilities in the popular Java-based logging library Log4j. By December 23, 2021, agencies were required to enumerate all solution stacks accepting data input from the internet; evaluate all software assets to determine whether Log4j was present in those assets; and take mitigation action. ED 22-02 was closed on April 8, 2022, and was replaced by BOD 22-01.
- **ED 22-03 - Mitigate VMware Vulnerabilities**: On March 18, 2022, ED 22-03 was issued in response to active exploitation of multiple vulnerabilities in several VMware products. ED 22-03 required FCEB agencies to identify impacted VMware products, deploy updates, or remove the product(s) from the agency network until an update could be applied. For instances of impacted VMware products that were accessible from the internet, agencies were to assume compromise, immediately disconnect from the production network, and conduct threat hunt activities.

Section II: Federal Cybersecurity Reporting and Analysis

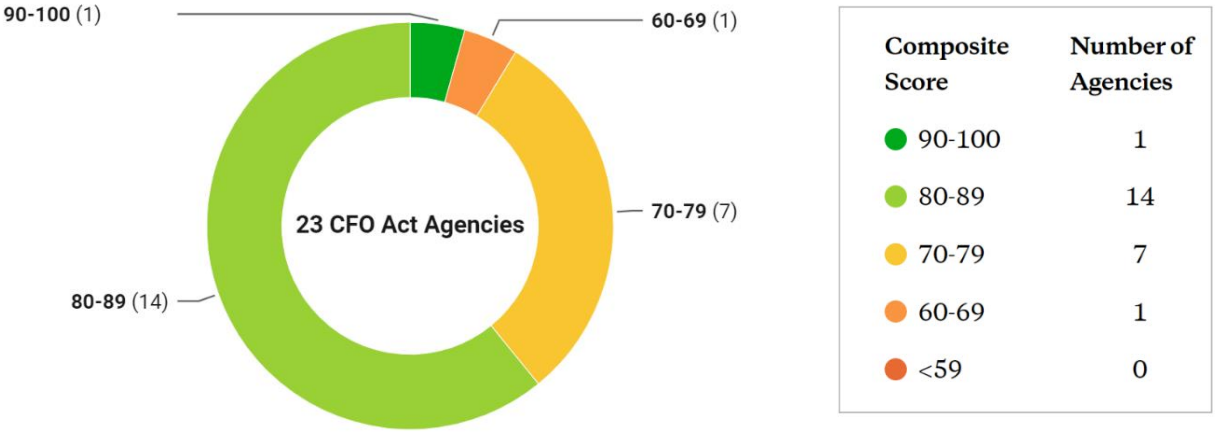
OMB leverages data as a strategic asset to increase the effectiveness of the Federal Government, facilitate oversight, and promote transparency. To this end, OMB publishes a portion of the data collected during the FISMA reporting process to the public; this section of the report includes findings based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

A. Tracking Progress in Zero Trust Architecture Adoption

Cybersecurity Progress Report

In FY 2022, OMB used the FISMA CIO metrics to track agency progress in implementing EO 14028 and subsequent policy guidelines. OMB evaluates agency submitted data to oversee agency information security policies and practices. To show agency progress throughout FY 2022 in implementing EO 14028 and related policy guidance, in December 2022, OMB published Federal Cybersecurity Progress Reports on performance.gov. 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.[5] Data derived from agency responses to annual FISMA CIO 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



The average score among 23 CFO Act agencies was 81 (out of a possible 100); one agency received a score of 94; fourteen agencies received scores between 80-89; seven agencies received scores between 70-79; and one agency scored 68. Progress report data also show that agencies are ready to assess and respond to cyber incidents. Over the course of the last year, every agency worked to evaluate CISA's Cybersecurity Incident and Vulnerability Response Playbooks against their current

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

incident response procedures and determined a process for sharing incident details electronically with CISA. Agencies have made great strides in executing key Administration cybersecurity priorities to reduce risk to the Federal Government, but the progress reports also make clear that large-scale change as envisioned in EO 14028 requires continued investment, collaboration, and cultural change.

Independent Assessments[6]

FISMA requires an agency's inspector general (IG), or an independent external auditor[7] to conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. Each year these independent assessors report on metrics (IG FISMA Metrics)[8] 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 M-22-05, *Fiscal Year 2022 Guidance on Federal Information Security and Privacy Management Requirements*, and the IG FISMA Metrics, a finding of *Managed and Measurable* (Level 4) is considered to be effective at the domain, function, and overall level. 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 2022, OMB implemented a new framework for both the timing and focus of IG assessments. The goal of the new framework is to provide a more flexible 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, represent important activities conducted by security programs, and contribute to the overall evaluation and determination of security program effectiveness.

IGs were instructed to focus only on the Core Metrics for FY 2022 during the transition to the new yearly evaluation cycle. The new cycle ended on July 31, 2022. Moving forward, IGs will continue to evaluate the Core Metrics on an annual basis and Supplemental Metrics at least once every two years.

Table 2 shows the number (and percentage) of agencies determined to have an effective information security program from FY 2017 to FY 2022. The percentage of agency information security programs evaluated as effective improved from 48 percent in FY 2017 to 64 percent in FY 2021. FY 2022 saw a

[6] 44 USC § 3553(c)(3) requires a summary of the independent evaluations; a summary of the IG/independent assessment can be found in each agency's one-pager.
[7] 44 USC § 3555(b).
[8] The FY 2022 IG FISMA Metrics are available at CISA's website.

slight decrease in security programs evaluated as effective, down to 61 percent. This change in trend was expected as IG evaluations were limited exclusively to the Core Metrics in FY 2022.

Table 2 IG Information Security Effectiveness Ratings

	FY17	FY18	FY19	FY20	FY21	FY22
Number of agency information security programs rated as overall "Effective"	**39** (48%)	**43** (51%)	**45** (54%)	**52** (60%)	**55** (64%)	**51** (61%)

Source: *Independent assessments of information security programs based on annual IG FISMA Metrics, representing 81 agencies in FY22*

B. FY 2022 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.

US-CERT Incidents by Vector

Agencies must classify incidents by method of compromise or data loss as part of their reporting requirements.[9] These data provide insight into the threats agencies face every day, allowing for a better understanding of the risks to Federal systems and data.

Table 3 shows 30,659 incidents reported by Federal agencies across nine categories, which represents a 5.7 percent decrease from the 32,543 incidents reported in FY 2021. While the trend is encouraging, drawing conclusions based on this data point, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years, would be premature.

For FY 2022, the "Other/Unknown" vector accounted for the highest number of reported incidents – 12,489, or roughly 41 percent of total incidents. The prevalence of this attack vector suggests additional rigor must be applied by agencies to appropriately categorize the vector of incidents during reporting, and when applicable, update the initial report when the vector is identified during the investigation process. Per M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, CISA will 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.

"Improper Usage" was the second most prevalent vector, with 10,467 incidents, or roughly 34 percent of total incidents. These data suggest that although agencies have processes or capabilities that

[9] 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.

detect when a security policy is being violated, many lack automated enforcement or prevention mechanisms.

Table 3 Agency-Reported Incidents by Attack Vector

Vector	FY21			FY 22		
	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.*	435	5	440	190	7	197
E-mail/Phishing *An attack executed via an email message or attachment.*	2,936	24	2,962	2,991	19	3,010
External/Removable Media *An attack executed from removable media or a peripheral device.*	15	0	15	46	1	47
Impersonation/Spoofing *An attack involving replacement of legitimate content/services with a malicious substitute.*	272	0	272	35	0	35
Improper Usage *Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.*	9,875	248	10,123	10,280	187	10,467
Loss or Theft of Equipment *The loss or theft of a computing device or media used by the organization.*	989	82	1,071	1,708	78	1,786
Web *An attack executed from a website or web-based application.*	2,722	8	2,730	2,445	8	2,453
Other/Unknown *An attack method does not fit into any other vector or cause of attack is unidentified.*	14,014	791	14,805	11,971	518	12,489
Multiple Vectors *An attack that uses two or more of the above vectors in combination.*	90	3	93	173	2	175
Total	**31,348**	**1,161**	**32,509**	**29,839**	**820**	**30,659**

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.[10] 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 2021 and FY 2022..

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

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 91 percent in FY 2021 and 93 percent in FY 2022) were considered "baseline," meaning that per the Cybersecurity Incident Severity Schema, they are considered "unsubstantiated or inconsequential event[s]."

Table 4 Agency-Reported Incidents by NCISS Priority Level

NCISS Priority Level	FY21	FY22
Uncategorized *Insufficient information was collected in order to provide an NCISS priority level.*	2,384	1,670
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.*	16,783	16,511
Baseline – Minor (Blue) *Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	12,766	12,205
Low (Green) *Unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	593	493
Medium (Yellow) *May affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.*	14	2
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.*	3	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	**32,543**	**30,881**[11]

Major Incidents

Of the incidents reported by agencies in FY 2022, four were determined by agencies to meet the threshold for major incidents in accordance with the definition in M-22-05. The U.S. Department of State reported a classified major incident in early 2022 that remains classified. A classified annex is available by request.

[11] Includes entities outside of the Federal executive branch.

Table 5 Summary of FY22 Major Incidents

Department of Agriculture *The United States Department of Agriculture (USDA) reported a major incident involving Personally Identifiable Information (PII) due to a process failure at the National Finance Center (NFC), a shared service provider for financial management and human resource management services for Federal agencies. NFC performed a manual feed to the Payroll and Personnel System that did not account for employee address changes. This resulted in 69,708 W-2C forms being generated and sent out through bulk physical mail.* *The W-2Cs included the employee's full name, unmasked full social security number (SSN), home address, wages, and employer information. Those impacted have been notified and offered free credit monitoring. Following this incident, NFC has made modifications, masking social security numbers on the W-2Cs, enhancing their systems to ensure addresses are in sync when W-2Cs are generated, and providing organization-wide PII training.*
Department of Education *The Department of Education reported a major incident involving the breach of personally identifiable information (PII) involving a loan servicing vendor's system. Beginning in June of 2022, a non-state criminal actor began attacking a web application, leveraging a vulnerability on a vendor-operated loan registration website. The attacker maintained a presence on the system until July 2022 when the activity was detected and the system was immediately shutdown.* *Following the incident, the vendor took mitigating steps to harden their systems through implementation of additional user validations and penetration testing exercises. Notification and credit monitoring services were offered to potentially affected individuals.*
Department of Treasury *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.*

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)[12] 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 66 non-CFO Act agencies on FY 2022 SAOP FISMA performance measures.

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).[13]

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

FY 2022 – SAOP FISMA Performance Measures[14]	CFO	Non-CFO
The head of the agency has designated an SAOP.[15]	100%	100%

[12] "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." OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) [hereinafter "OMB Circular A-130"], § 10(a)(57).

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

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

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

Among the agencies that have designated an SAOP:		
The SAOP has the necessary role and responsibilities within the agency for compliance.[16]	100%	98%
The SAOP has the necessary role and responsibilities within the agency for policy making.[17]	100%	98%
The SAOP has the necessary role and responsibilities within the agency for risk management activities.[18]	100%	97%
The agency has developed and maintained a privacy program plan.[19]	100%	88%
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.[20]	100%	93%

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.

Table 7 Personally Identifiable Information Inventory

FY 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains an inventory of the agency's information systems[21] that handle PII.[22]	100%	97%

[16] *See id.*
[17] *See id.*
[18] *See id.*
[19] 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).
[20] *See id*. at Appendix I § 4(b)(1).
[21] 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).
[22] *See* OMB Circular A-130 at § 5(a)(1)(a)(ii), 5(f)(1)(e).

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 2022 – 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.[23]	100%	90%
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%	89%
The agency has developed and implemented a written policy to help ensure that any new collection or use of SSNs is necessary.	100%	77%
Among the agencies with such written policies:		
The agency's written policy provides specific criteria to use when determining whether the collection or use of SSNs is necessary.	100%	92%
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%	90%
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.[24]	96%	86%

[23] 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.
[24] *See* OMB Circular A-130 at § 5(f)(1)(f).

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 2022 – 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.[25]	100%	98%
Selection, implementation, and assessment of privacy controls.[26]	100%	93%
Authorization of information systems and common controls.[27]	100%	95%
Continuous monitoring of information systems that process PII.[28]	100%	88%
The agency has designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls.[29]	96%	73%
The agency has developed and maintained a written privacy continuous monitoring strategy.[30]	92%	74%
The agency has established and maintained an agency-wide privacy continuous monitoring program.[31]	88%	65%

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

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 2022 – 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.[32]	3,866	472
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.[33]	76%	93%
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.[34]	71%	78%
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.[35]	72%	76%
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	78%	87%

[32] 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).
[33] *See id*. at Appendix I § 4(a)(2), 4(e)(7).
[34] 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).
[35] *See id*. at Appendix I § 4(e)(3).

risks, prior to the authorizing official making a risk determination and acceptance decision.[36]		

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 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has a policy that includes explicit criteria for analyzing privacy risks when considering IT investments.[37]	92%	68%
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.[38]	83%	68%
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,

[36] *See id.* at Appendix I § 4(e)(9).
[37] *See id.* at § 5(d)(3).
[38] *See id.* at § 5(a)(3)(e)(ii).

security officials, counsel, and other relevant agency officials in order to conduct a meaningful assessment.

Table 12 Privacy Impact Assessments

FY 2022 – 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.	4,975	837
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.[39]	81%	87%
Among the agencies that have a written policy for PIAs, the written policy for PIAs includes:[40]		
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%	96%
The agency has a process or procedure for:[41]		
Assessing the quality and thoroughness of each PIA.	100%	79%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	100%	80%
Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated.	96%	79%

[39] 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).
[40] *See id.* at Appendix II § 5(e) (July 28, 2016).
[41] *See* OMB Circular A-130 at Appendix II § 5(e).

	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%	76%

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 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency ensures that the agency's privacy workforce has the appropriate knowledge and skill.[42]	96%	98%
The agency has assessed its hiring, training, and professional development needs with respect to privacy during the reporting period.[43]	88%	94%
The agency has developed a workforce planning process to ensure that it accounts for privacy workforce needs.[44]	75%	76%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions.[45]	75%	79%

Table 14 Training and Accountability

FY 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency provides foundational privacy training to its Federal employees (including managers and senior executives).[46]	100%	95%

[42] *See* OMB Circular A-130 at § 5(c)(2).
[43] *See id.* at § 5(c)(6).
[44] *See id.* at § 5(c)(1).
[45] *See id.*
[46] *See id.* at Appendix I § 4(h)(4); *see also id.* at Appendix I § 4(h)(1).

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.[47]	83%	59%
The agency has ensured that measures are in place to test the knowledge level of information system users in conjunction with privacy training.[48]	96%	85%
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.[49]	100%	100%
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.[50]	100%	95%

Table 15 Contractors and Third Parties

FY 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors.[51]	100%	92%
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.[52]	100%	98%
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.[53]	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:[54]		

[47] *See id.* at Appendix I § 4(h)(5); *see also id.* at Appendix I § 4(h)(1).
[48] *See id.* at Appendix I § 4(h)(4).
[49] *See id.* at Appendix I § 4(h)(6).
[50] *See id.* at Appendix I § 4(h)(7).
[51] *See id.* at Appendix I § 4(h)(1), (4)-(5).
[52] *See id.* at Appendix I § 4(h)(6).
[53] *See id.* at Appendix I § 4(h)(7).
[54] *See id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).

Processes do not exist.	0%	0%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	13%	30%
Processes are fully documented and implemented and cover all relevant aspects.	8%	27%
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%	42%
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:[55]		
Processes do not exist.	0%	0%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	4%	26%
Processes are fully documented and implemented and cover all relevant aspects.	17%	23%
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%	52%

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.[56]

Table 16 Breach Response

FY 2022 – SAOP FISMA Performance Measures	CFO	Non-CFO

[55] *See id.* at Appendix I § 4(j)(2)(a).

[56] *See* OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).

Among the agencies that have a breach response plan, the breach response plan includes the agency's policies and procedures for:[57]		
Reporting a breach	100%	100%
Investigating a breach	100%	100%
Managing a breach	100%	98%
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.[58]	100%	92%
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.[59]	100%	95%
Among the agencies with a breach response team, all members of the agency's breach response team participated in at least one tabletop exercise during the reporting period.[60]	71%	58%
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that were reported within agencies during the reporting period.[61]	18,409	1,402
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.[62]	11,410	82
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that agencies reported to Congress as major incidents (as defined in OMB Memorandum M-22-05) during the reporting period.[63]	3	0
The total number of individuals potentially affected by the breaches reported to Congress as major incidents during the reporting period.[64]	3,578,141	Not applicable

[57] *See id.* at § VII, XI.
[58] *See id.* at § X.B, XI.
[59] *See id.* at § VII.A, XI.
[60] *See id.* at § X.A, XI.
[61] *See id.* at § III.C, XI.
[62] *See id.* at § VII.D.1, XI.
[63] *See id.* at § VII.D.3, XI.
[64] *See id.* at § 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 in FY 2022 Core IG FISMA 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*