



# Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2021

*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 the intrusion detection and prevention capabilities, as required by the Cybersecurity Act of 2015, Pub. L. No. 114-113, § 226(c)(1)(B), and incorporates agency reporting on complying with privacy requirements and managing 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 2021 data reported by agencies to OMB and DHS.*

# Table of Contents

Executive Summary: The State of Federal Cybersecurity	5
Section I: Federal Cybersecurity Activities	6
A.    Building a Modern Cybersecurity Infrastructure	6
Office of the National Cyber Director (ONCD)	6
Executive Order 14028 (EO 14028)	6
B.    Programs and Policy Areas	7
Continuous Diagnostics and Mitigation (CDM)	7
National Cybersecurity Protection System (NCPS)	8
Coordinated Vulnerability Disclosure (CVD)	10
High Value Assets (HVAs)	10
Trusted Internet Connections (TIC)	12
Supply Chain Risk Management	12
Binding Operational Directives (BODs) and Emergency Directives (EDs)	13
Section II: Federal Cybersecurity Reporting and Analysis	15
A.    Improvements in Cybersecurity Hygiene	15
Cybersecurity Cross-Agency Priority (CAP) Goal Performance	15
Risk Management Assessments (RMAs)	18
Independent Assessments	19
B.    FY 2021 Information Security Incidents	21
Incidents by Vector	21
Incidents by NCISS Priority Level	24
Major Incidents	27
C.    Cybersecurity Risk Management	28
Integration of Cyber and ERM Programs	28
FY2021 Priority IG Metrics Pilot	29
Supply Chain Risk Management IG Assessment	31
Overall Cyber Risk Management Summary	32
Section III: Senior Agency Official for Privacy (SAOP) Performance Measures	33

A.	Senior Agency Officials for Privacy (SAOPs) and Privacy Programs	33
B.	Personally Identifiable Information and Social Security Numbers	34
C.	Privacy and the Risk Management Framework	36
D.	Information Technology Systems and Investment	39
E.	Privacy Impact Assessments	40
F.	Workforce Management	41
G.	Breach Response and Privacy	44
	Appendix I: Agency Cybersecurity Performance Summaries	47
	CIO Self-Assessments and CIO Ratings	47
	Independent Assessments and IG Ratings	48
	Appendix II: Commonly Used Acronyms	49

# Executive Summary: The State of Federal Cybersecurity

President Biden took office in January 2021, amid an unprecedented series of large-scale cyber-attacks against software supply chains, key Federal systems, and critical infrastructure. Fiscal Year (FY) 2021 began with the discovery of the SolarWinds software supply chain attack that had been ongoing since FY 2020. A series of Microsoft Exchange Server attacks was discovered less than 2 months after President Biden's inauguration, and that was followed by the Colonial Pipeline ransomware attack. By the end of FY 2021, Federal agencies had reported a 6% increase in cyber incidents when compared against those reported in FY 2020.

The President responded quickly by moving to strengthen our cybersecurity posture through a series of bold actions. These actions included Executive Order (EO) 14028, as well as a series of subsequent actions by the Office of Management and Budget (OMB), the National Security Council (NSC), and the Cybersecurity and Infrastructure Security Agency (CISA) to protect our digital infrastructure. EO 14028, in particular, represents a paradigm shift for the U.S. Government and recognizes that previous approaches to securing Federal systems have been insufficient.

Implementation of EO 14028 has upgraded the security posture of Federal civilian executive branch (FCEB) agencies. Leading security practices like zero trust architecture (ZTA), phishing-resistant multi-factor authentication (MFA), and secure software development frameworks are now core parts of FCEB agencies' digital security strategies.

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

## FY 2021 Report Key Takeaways:



32,543 incidents were reported in FY 2021 (6% increase over previous year). Seven were reported as major incidents, several related to the SolarWinds attack.



Agencies show improvements in cyber hygiene; however, more work is necessary.



Agencies continue to work with private sector partners to mitigate cyber attacks and reduce the risk to federal infrastructure.

# Section I: Federal Cybersecurity Activities

## A. Building a Modern Cybersecurity Infrastructure

### Office of the National Cyber Director (ONCD)

The Office of the National Cyber Director (ONCD) within the Executive Office of the President was created in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283) to advise the President on cybersecurity and related emerging technology issues and to coordinate the implementation of national cybersecurity strategy and policy. On June 17, 2021, the Senate confirmed Chris Inglis to serve as the first National Cyber Director of the United States. Establishing and standing up ONCD demonstrates the Administration’s commitment to building a coherent and unified approach to cybersecurity. ONCD serves as a focal point for ensuring the Government is speaking with one voice, moving in the same direction, and, to the greatest extent practicable, sharing common priorities by which we can organize our collective efforts for maximum possible effect.

ONCD, in partnership with OMB, will support departments and agencies as they continue to implement EO 14028, to include planning for the future of their cyber needs, assessing the performance of relevant programs in achieving their intended effect, and championing successful approaches. ONCD will also play a role in planning and incident response, technology and ecosystem security, workforce development, and stakeholder engagement as it impacts Federal cybersecurity.

### Executive Order 14028 (EO 14028)

In May 2021, President Biden issued the Executive Order 14028 (EO 14028), *Improving the Nation’s Cybersecurity*. This Executive Order makes a significant contribution towards modernizing Federal cybersecurity defenses by protecting Federal systems, improving information-sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States’ ability to respond to incidents when they occur. Foundationally, this Executive Order recognizes the hard truth: “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.”

EO 14028 challenges Federal agencies to aggressively change the security strategy and culture across the Federal enterprise to center on cutting-edge practices in the cybersecurity community. Departments and agencies must move beyond the concept of defending a large network perimeter against cyber threats while placing implicit trust in internal networks and system components. Instead, agencies must assume their perimeter defenses can—and ultimately will—be compromised. Agencies must therefore limit access through secure, phishing-resistant identity authentication, build modern protections into the applications

that hold Federal data, and increase capabilities for detection and response across both systems and endpoints. The Executive Branch must work with Congress to invest in secure solutions to make our Federal systems resilient against the current cyber threats we face. Federal agencies are now working to implement the Executive Order by expanding MFA and encryption of data, leveraging endpoint detection and response, and expanding logging of critical data to support rapid investigations when Federal agencies suspect a system may have been compromised.

## **B. Programs and Policy Areas**

### **Continuous Diagnostics and Mitigation (CDM)**

The Continuous Diagnostics Mitigation (CDM) program at the Department of Homeland Security (DHS) was developed in 2012 to support efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect Federal civilian systems across all organizational tiers. The CDM program provides Federal agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis. This enhances agencies' ability to prioritize cybersecurity risks and enables cybersecurity personnel to mitigate the most significant problems first. The CDM program will also provide 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. The 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.

To further support the CDM program, [OMB Memorandum M-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements](#), requires Federal agencies to provide sufficient justification prior to purchasing and using tools purchased outside of the CDM program's acquisition vehicles. M-21-02 provides that CISA will fund agencies' initial procurement of tools through the CDM program, as well as the first year of operations and maintenance (e.g., licensing) costs. After the first year, Federal agencies subject to the Chief Financial Officers Act of 1990 (CFO Act), Pub. L. No. 101-576, must fund long-term operations and maintenance of their CDM-related tools. Additionally, Federal agencies must show these CDM-specific line items in their annual congressional budget justification documents, as applicable. M-21-02 further specifies that the CDM Program Management Office (PMO) will cover licensing costs for CDM tools for certain agencies that are not covered by the CFO Act (non-CFO Act agencies). The memorandum also requires agencies to take various steps to improve the quality of the data they provide to the Federal CDM dashboard. By June 2021, the CDM program had provided services to 36 agencies, and it

is projected to provide services to 50 agencies by the end of FY 2022.<sup>1</sup> Over the course of FY 2021, the program matured its “Shared Services Platform (SSP) 2.0,” through which it delivers services to Federal agencies, by:

- Rapidly validating and adding two EDR technologies to the catalog of security capabilities. These solutions aligned with requirements in EO 14028 and were made available to agencies prepared to implement these toolsets.
- Deploying and successfully rolling out enhanced asset management capabilities to agencies, which increased vulnerability-management functionality.
- Per M-21-02, certifying the first set of non-CFO act agencies in the CDM program’s data quality management plan, fully implementing the asset management capabilities at these agencies and making them ready to automate cyber reporting.
- Initiating development of mobile security capabilities – including Enterprise Mobility Management and Mobile Threat Detection.

The FISMA FY 2022 report will provide additional detail on the progress of this program. As part of CDM, CISA deployed a privileged access management (PAM) tool to transition 30 disparate information systems into a cohesive enterprise-wide approach.

### National Cybersecurity Protection System (NCPS)

CISA’s National Cybersecurity Protection System (NCPS) provides a suite of tools to enhance the boundary awareness and security of Federal agencies. The most recent addition to these capabilities offered by NCPS is EINSTEIN 3 Accelerated (E3A), an integrated intrusion prevention, detection, and analysis system that builds on the passive detection capabilities of EINSTEIN 1 and EINSTEIN 2. The E3A program aggregates FCEB traffic, enabling the deployment of new and advanced protections by CISA. Table 1 demonstrates the implementation status as of October 1, 2021.

---

<sup>1</sup> <https://www.cisa.gov/sites/default/files/publications/cdm-program-overview-fact-sheet-012022-508.pdf>



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

EINSTEIN Capability	● Complete		◐ In Progress		◑ Deferred <sup>2</sup>		✗ Not Implemented	
	2020	2021	2020	2021	2020	2021	2020	2021
<b>E1/E2</b>	<b>80</b>	<b>82</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>28</b>	<b>21</b>
CFO	23	23	0	0	0	0	0	0
Non-CFO	57	59	0	1	0	0	28	21
<b>E3A Email</b>	<b>81</b>	<b>82</b>	<b>5</b>	<b>3</b>	<b>3</b>	<b>5</b>	<b>18</b>	<b>14</b>
CFO	23	23	0	0	0	0	0	0
Non-CFO	58	59	5	3	3	5	18	14
<b>E3A DNS</b>	<b>86</b>	<b>87</b>	<b>1</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>15</b>	<b>13</b>
CFO	23	23	0	0	0	0	0	0
Non-CFO	63	64	1	1	2	3	15	13

As the Federal Government shifts away from perimeter-based defenses and adopts a zero-trust architecture, new toolsets must be adopted to detect and respond to increasingly sophisticated threat activity on Federal systems. Per EO 14028, Federal departments and agencies are rapidly deploying Endpoint Detection and Response (EDR) capabilities to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

These EDR toolsets are being integrated with the NCPS program 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

<sup>2</sup> These agencies face a technical challenge to implement email filtering for its third party, cloud-based email service. CISA continues to work with the affected agencies and their E3A service provider to engineer solutions.

transition is part of a recognition that every device that connects to a network is a potential attack vector for cyber threats. CISA, the Chief Information Officer (CIO) Council, and IT leadership across departments and agencies will ensure these deployments are integrated into the Federal security strategy over the coming year; the FY 2022 report will provide additional detail on EDR deployment progress.

### Coordinated Vulnerability Disclosure (CVD)

Coordinated Vulnerability Disclosure (CVD) enables agencies to improve their information security programs by welcoming cybersecurity review from outside researchers. In FY 2020, OMB issued [OMB Memorandum M-20-32, \*Improving Vulnerability Identification, Management, and Remediation\*](#), and CISA issued binding operational directive [BOD-20-01, \*Develop and Publish a Vulnerability Disclosure Policy\*](#), which together required agencies to solicit and review vulnerability findings from the general public. In FY 2021, agencies published their Vulnerability Disclosure Policies on their primary .gov websites and developed implementation plans providing timelines and milestones for those policies. CVD is among the most effective methods for obtaining new insights into security vulnerabilities and understanding one's external risk posture, which provides high return on investment. CVD policies also provide protection for those who uncover these vulnerabilities by explicitly authorizing good-faith security research.

### High Value Assets (HVAs)

HVAs are assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification or destruction could cause significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.<sup>3</sup> The assessments of HVA systems show the Federal Government continued to face challenges in mitigating basic security vulnerabilities on these critical systems in FY 2021. The most common security deficiencies identified across the HVA landscape are identified in Figure 1.

In December 2018, OMB expanded the HVA program to support all agencies, including both CFO Act and non-CFO Act agencies. The HVA program supports the identification of these assets, assessment to identify areas of weakness, remediation of those concerns, and response to incidents.

The CISA HVA PMO plans, prioritizes, and coordinates delivery of cybersecurity services to assist Federal agencies in identifying and managing their HVAs and to better enable the

---

<sup>3</sup> M-19-03.

identification and risk assessment of the overall Federal HVA enterprise. The HVA Program’s cybersecurity service portfolio includes, but is not limited to:

- Security Architecture Review (SAR): a collaborative evaluation of an agency’s HVA Cyber Security posture, inclusive of the HVA and its underlying components;
- Risk and Vulnerability Assessment (RVA): a collaborative effort to assess the accessibility and Cyber Security posture of the HVA and its surrounding infrastructure;
- Federal Incident Response Evaluation (FIRE) with Security Operations Center (SOC) Module;
- Vulnerability Scanning Assessment (Cyber Hygiene Scans); and
- Red Team Assessment (RTA).

**Figure 1 Top 5 High Value Asset Assessment Findings in FY 2021**



Due to COVID-19, agencies expanded the availability of telework to employees and contractor personnel, and limited the number of individuals allowed inside their buildings and facilities. Therefore, CISA faced challenges conducting security architecture reviews (SAR) and vulnerability risk assessments (VRA). To reduce the number of visits to agencies and avoid backlogs, CISA’s HVA PMO revised the FY 2021 assessment process by combining the SAR and VRA into a single methodology. Using this new methodology, CISA conducted 46 total HVA assessments resulting in 263 findings in FY 2021. With COVID limitations, the overall number of assessments decreased by 24 percent when compared to FY 2020. The findings per assessment—and overall types of findings—were comparable between FY 2020 and FY 2021.

## Trusted Internet Connections (TIC)

On September 12, 2019, OMB updated the Trusted Internet Connection (TIC) policy in [OMB Memorandum M-19-26, \*Update to the Trusted Internet Connections \(TIC\) Initiative\*](#). The updated policy allows industry to propose, and agencies to adopt, new solutions to take advantage of modern internet capabilities.

Based on comments from the public, CISA updated six of their nine guidance documents for TIC 3.0 implementation during FY 2021.<sup>4</sup> These updates ensure consistent implementation approaches across all agencies. The new guidance offers agencies opportunities to securely modernize their enterprise environments as they migrate from legacy solutions to more agile and distributed architectures. It also encourages the adoption of zero trust principles. In addition, the guidance allows for agencies and industry to collaborate with CISA on improving visibility across the evolving Federal enterprise.

## Supply Chain Risk Management

The Federal Government faces challenges addressing the growing scale and complexity of securing the IT supply chain. In response, Congress enacted new legislation in 2018 to improve executive branch coordination, supply chain information sharing, and actions to address supply chain risks. The Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act, Pub. L. No. 115-390, requires agencies to assess the risks to their respective information and communications technology supply chains, such as through their Supply Chain Risk Management (SCRM) programs. The SECURE Technology Act also established the Federal Acquisition Security Council (FASC) to provide an interagency process through which the Federal Government can address potential security threats posed by hardware, software, systems, and devices related to information technologies and telecommunications equipment and services.

In August 2021, the FASC issued a final rule to implement the requirements of the laws that govern the operation of the FASC, the sharing of supply chain risk information, and the exercise of its authorities to recommend issuance of removal and exclusion orders to address supply chain security risks.<sup>5</sup> The rule includes procedures for the FASC to identify, evaluate, and address supply chain risks by making recommendations on potential exclusion and removal orders to the Secretaries of Defense and Homeland Security, as well as the Director of National Intelligence. The final rule also provides processes to issue removal and exclusion orders, along with agency waiver requests. These critical steps safeguard information and

---

<sup>4</sup> <https://www.cisa.gov/tic-guidance>

<sup>5</sup> 86 Fed. Reg. 47581

communication technology from emerging threats and support the establishment of SCRM standards for the acquisition community.

### Binding Operational Directives (BODs) and Emergency Directives (EDs)

Section 3553 of title 44, U.S. Code, 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 four EDs in FY 2021:

- **ED 21-01: Mitigate SolarWinds Orion Code Compromise:** On December 13, 2020, ED 21-01 required agencies to examine stored network traffic for indications of compromise for specific versions of SolarWinds Orion versions (2019.4 through 2020.2.1 HF1). Agencies were directed to power down affected versions of the product and conduct enumerated mitigations. ED 21-01 was updated on April 15, 2021, attributing responsibility for the SolarWinds Orion incident.
- **ED 21-02: Mitigate Microsoft Exchange On-premises Product Vulnerabilities:** On March 3, 2021, ED 21-02 was issued following observations by CISA partners of active exploitation of vulnerabilities in Microsoft Exchange on-premises products. CISA issued supplemental direction on March 31, 2021, and April 13, 2021. Depending on its level of expertise, each agency was instructed to take one of two courses of action. Agencies without expertise were required to immediately disconnect of Microsoft Exchange on-premises servers. Agencies with expertise were directed to examine artifacts for evidence of compromise or anonymous behavior. Recognizing exchange servers are a primary target for adversary activity, CISA provided agencies updated direction requiring further actions to implement additional security measures to reduce the risk to these systems.
- **ED 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities:** On April 20, 2021, ED 21-03 was issued after active exploitation of vulnerabilities in Pulse Connect Secure products, a widely used SSL (Secure Sockets Layer) remote access solution. Successful exploitation of these vulnerabilities could allow an attacker to place webshells on the appliance operating the vulnerable software to gain persistent system access. The directive required agencies to identify instances of Pulse Connect within 3 days, then deploy the Pulse Connect Secure Integrity Tool and continue to run the tool every 24-hours. In addition, agencies were required to implement reporting requirements and

update instances of Pulse Connect Secure with available patches within 48 hours of patch availability.

- **ED 21-04: Mitigate Windows Print Spooler Service Vulnerability:** On July 13, 2021, CISA issued ED 21-04 after it became aware of active exploitation of a vulnerability in the Microsoft Windows Print Spooler service. The actions agencies were required to take include disabling the print spooler device on all Microsoft Active Directory (AD) Domain Controllers (DC) within 1 day of the directive issuance, applying cumulative updates to all Windows servers and workstations within 7 days of issuing the directive, and further configuring Microsoft Windows operating systems other than domain controllers within those 7 days, as well.

# 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 that data.

## A. Improvements in Cybersecurity Hygiene

### Cybersecurity Cross-Agency Priority (CAP) Goal Performance

In 2018, OMB used requirements within the Government Performance and Results Modernization Act (GPRAMA) of 2010, Pub. L. No. 111-352, to track agency progress towards meeting cybersecurity goals. GPRAMA requires the Director of OMB to coordinate with agencies to develop priority goals to improve the performance and management of the Federal Government.<sup>6</sup> In the previous Administration, the President's Management Agenda established a Cross-Agency Priority (CAP) Goal to Modernize IT to Increase Productivity and Security. Included in this IT Modernization CAP Goal was a structure to reduce cybersecurity risks to the Federal mission by mitigating the risk and impact of threats to Federal agencies' data, systems, and networks by implementing cutting edge cybersecurity capabilities. The strategies to implement this structure included managing asset security, protecting data and networks, and limiting personnel access.<sup>7</sup>

To track agency progress, OMB required agencies to report certain FISMA CIO metrics related to these three areas as part of a data collection to track CAP Goal progress and posted the results on performance.gov. FY 2021 CIO FISMA metrics include performance targets on Information Security Continuous Monitoring (ISCM), Strong Authentication (ICAM), and Advanced Network and Data Protections (ANDP). The collection process is outlined in OMB Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. A summary of the Federal Government's overall performance on these cybersecurity metrics from FY 2017 to FY 2021 can be found below in Table 2. A majority of CFO Act agencies have met the goals established for these metrics, indicating the continuing improvement of information security hygiene.

The success of agencies in conducting certain cyber hygiene metrics shows they are meeting baseline security goals. However, the changing threat landscape for Federal networks is

---

<sup>6</sup> <https://www.govinfo.gov/content/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf>

<sup>7</sup> [https://assets.performance.gov/archives/action\\_plans/FY2018\\_Q1\\_IT\\_Modernization.pdf](https://assets.performance.gov/archives/action_plans/FY2018_Q1_IT_Modernization.pdf)

characterized by increasingly targeted and sophisticated attacks. This changing landscape led to a need to reevaluate how the Administration measures agencies' readiness to address today's risks. For example, by the end of FY2021, agencies had reached near-universal compliance with certain measures, such as mobile device management.<sup>8</sup> Focusing on baseline compliance activities where agencies had already achieved success obscured the areas most in need of attention.

In order to ensure the Administration focuses oversight and resources on the most critical security gaps, OMB eliminated FISMA metrics that required agencies to provide pro forma documentation and adjusted others to meet core cybersecurity needs, including the need to track implementation of zero trust architectures across the Federal enterprise. To gauge agency progress in defending against the realities of this threat landscape, OMB established new reporting requirements that address the tactics and techniques being leveraged by our adversaries against Federal systems. The [FY2022 CIO FISMA Metrics](#), along with OMB Memorandum M-22-05, [Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements](#), marked this shift in strategic direction. By issuing that guidance, OMB ensures agencies are focused on zero trust architectures, ground truth testing, the use of observable security outcomes, an increased focus on automation, and the overall need to align protections with the modern threat landscape.

---

<sup>8</sup> <https://trumpadministration.archives.performance.gov/data/#cap>



**Table 2 FY 2017 - FY 2021 CAP Goal Metric Summary**

CAP Goal Metric	Target	Number of Agencies Meeting Target					Average Implementation*				
		FY 17	FY 18	FY 19	FY 20	FY 21	FY 17	FY 18	FY 19	FY 20	FY 21
<b>Manage Asset Security</b>											
Hardware Asset Management	95%	58	71	73	75	80	67%	64%	70%	85%	82%
Software Asset Management	95%	53	56	70	78	79	69%	58%	75%	85%	86%
Authorization Management**	100%	51	79	81	77	77	84%	91%	94%	94%	95%
Mobile Asset Management	95%	N/A	78	89	90	89	N/A	96%	99%	99%	99%
<b>Limit Personnel Access</b>											
Privileged Network Access Management	100%	46	56	58	61	62	93%	94%	96%	96%	94%
High Value Asset System Access Management**	90%	N/A	58	66	71	70	N/A	70%	75%	81%	83%
Automated Access Management	95%	N/A	63	67	72	77	N/A	63%	88%	92%	93%
<b>Protect Networks and Data</b>											
Intrusion Detection and Prevention	4 of 6	N/A	45	60	75	73	N/A	N/A	N/A	N/A	N/A
Exfiltration and Enhanced Defenses	90%	N/A	66†	79	79	83	N/A	N/A	N/A	N/A	N/A
Data Protection**	4 of 6	N/A	67	75	81	88	N/A	N/A	N/A	N/A	N/A

Source: CAP Goal Metrics [FY 2021 FISMA CIO Metrics \(calculations described in Appendix A\)](#) representing 96 agencies in FY 2021 and previous annual FISMA reports.

\* OMB used a weighted average of applicable assets or users to determine the Government-wide average.

\*\* Small agencies that do not report HVAs or have high or moderate impact systems are not considered in weighted average.

† In FY 2018, the vast majority of agencies (93, including all 23 civilian CFO Act agencies) have met 3 of the 4 original targets set in the Exfiltration and Enhanced Defenses CAP goal. Accordingly, OMB considered those targets to be

achieved and shifted focus to the remaining metric, concerning exfiltration detection (FISMA CIO Metric 3.8). This figure represents the number of agencies meeting the target for that metric in FY 2018.

---

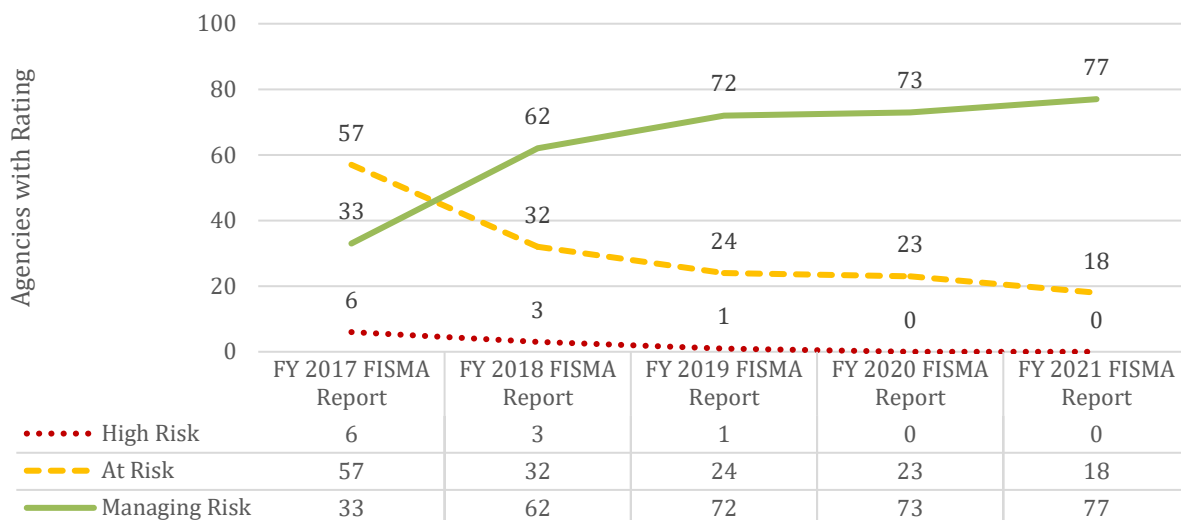
## Risk Management Assessments (RMAs)

[OMB Memorandum M-17-25, Reporting Guidance for Executive Order Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#), established the Risk Management Assessment (RMA) cybersecurity scorecard process for agencies. While the reporting towards the IT Modernization CAP goal has focused on a handful of metrics, the RMA covers a larger set of information security controls and capabilities in alignment with the NIST Cyber Security Framework (CSF).

In FY 2017 six agencies received a rating of “High Risk” (the poorest rating), with 33 agencies receiving the rating of “Managing Risk” (the best rating). As of FY 2021 reporting, no agencies received a rating of “High Risk,” and 77 agencies received a rating of “Managing Risk.” A summary of the RMA ratings from FY 2017 to FY 2021 can be found below in Figure 2, based on responses from 95 agencies in FY 2021.

In FY 2021, OMB continued to improve cybersecurity processes to align with the Administration’s priorities, agency risk profiles, and the ever-evolving threat environment by applying lessons learned from past RMA processes. The FY 2021 Inspector General (IG) FISMA Reporting Metrics include a new domain on SCRM within the identify function. This new domain focuses on the maturity of agency SCRM strategies, policies, procedures, plans, and processes to make sure products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain risk management requirements. The IG FISMA Reporting Metrics also include a new question that measures the degree to which agencies utilize vulnerability disclosure policies as part of their vulnerability management program for internet-accessible Federal systems. In addition, the IG metric questions related to the implementation of policies and procedures were reorganized and streamlined to reduce redundancies.

**Figure 2 Agency Risk Management Assessment (RMA) Ratings**



Source: RMA ratings based on [FY 2021 FISMA CIO Metrics](#) representing 95 agencies in FY 2021 and previous annual FISMA reports.

Note: 2 Non-CFO Act agencies did not report in 2021 and a non-CFO Act agency began reporting in 2021

### Independent Assessments<sup>9</sup>

FISMA requires an agency’s IG, if there is one, or an independent external auditor<sup>10</sup> 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)<sup>11</sup> 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 Cyber Security Framework is assessed using a five-level maturity model.

Pursuant to OMB M-20-04 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

<sup>9</sup> 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.

<sup>10</sup> 44 USC § 3555(b)

<sup>11</sup> The FY 2021 IG FISMA Metrics are available at CISA’s [website](#).

to determine the effectiveness of their agencies' cybersecurity programs. Table 3 shows the number (and percentage) of agencies determined to have an effective information security program from FY 2017 to FY 2021. The percentage of agency information security programs evaluated as effective improved from 48% to 64%.

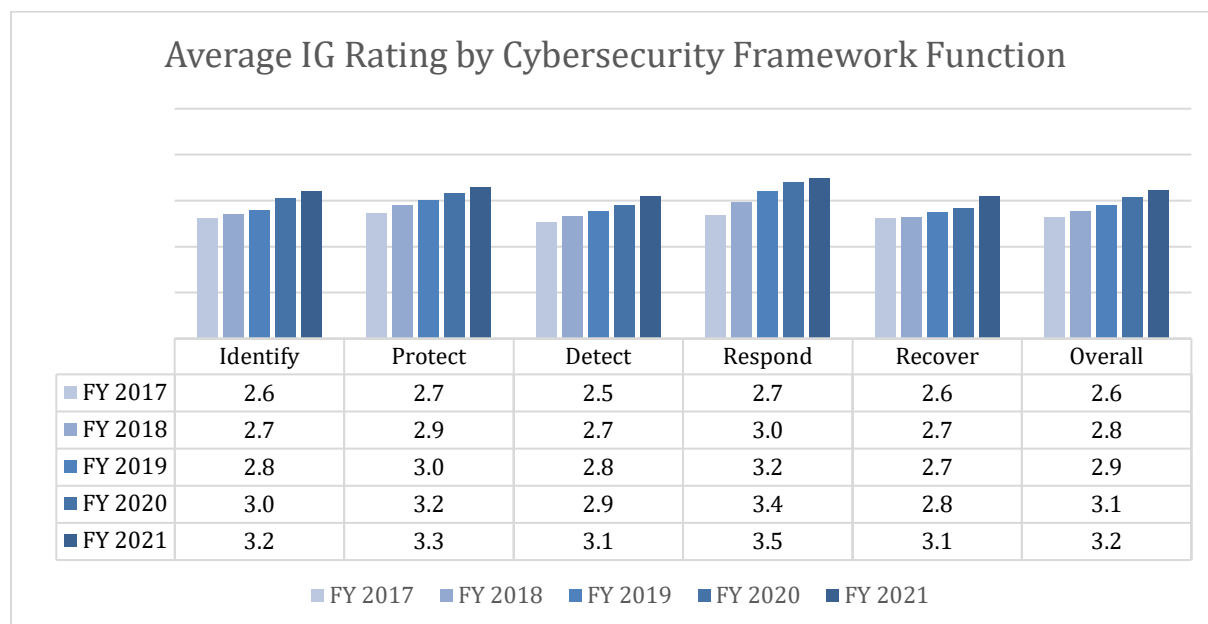
**Table 3 IG Information Security Effectiveness Ratings**

IG Metric	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021
Number of agency information security programs rated as overall "Effective" by their independent assessment, based on applicable OMB guidance	39 (48%)	43 (51%)	45 (54%)	52 (60%)	55 (64%)

Source: Independent assessments of information security programs based on annual IG FISMA Metrics, representing 86 agencies in FY 2021

Figure 3 depicts agencies' ratings for each function of NIST's Cyber Security Framework from FY 2017 to FY 2021, across 86 agencies (in FY 2020) weighted equally. The average rating for each function improved from 2.6 (above the threshold for *Defined* on the maturity scale) to 3.2 (above the threshold for *Consistently Implemented* on the maturity scale). Taken together, these metrics indicate that agencies have continued to make steady progress in improving their information security programs.

**Figure 3 IG Average NIST Cybersecurity Framework (CSF) Function Rating Levels**



Source: Unweighted average rating (out of 5) for each NIST CSF Function based on independent assessments using annual IG FISMA Metrics; the FY 2021 number reflects the ratings of 85 agencies. SCRM was excluded from this table to allow for consistent measurement across five years. An analysis of the SCRM function can be found in Section II.C of this report.

## B. FY 2021 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 a 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.

### Incidents by Vector<sup>12</sup>

Agencies must classify incidents by method of compromise or data loss as part of their reporting requirements.<sup>13</sup> This data provides visibility into the threats agencies face every day, allowing for a better understanding of the risks to Federal systems and data. The Agency

<sup>12</sup> 44 USC § 3553(c)(1).

<sup>13</sup> 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>.










Cybersecurity Performance Summaries in Appendix I include additional detail for individual agencies.

Table 4 shows 32,543 incidents reported by Federal agencies and validated with CISA across nine categories, representing a 6% increase from the 30,819 incidents reported in FY 2020. Of the reported incidents, 34 were reported by non-FISMA entities while 32,509 were from CFO/non-CFO act agencies. The growing number of incidents continues to indicate that cybersecurity requires constant vigilance.

For FY 2021, the “Other/Unknown” vector accounted for the highest number of reported incidents—14,014 incidents, about 43%. 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 unveiled during the investigation process. OMB and CISA continue to work with agencies to improve the quality of incident reporting data.

“Improper Usage” was the second most common vector, with 9,875 incidents (approximately 30.3%). The prevalence of this vector indicates that, although agencies have processes or capabilities that detect when a security policy is being violated, many lack automated enforcement or prevention mechanisms.

**Table 4 Agency-reported Incidents by Vector**

Vector	FY 20			FY 21		
	CFO	Non-CFO	Gov-wide	CFO	Non-CFO	Gov-wide
 <b>Attrition</b> An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	342	3	345	435	5	440
 <b>E-mail/Phishing</b> An attack executed via an email message or attachment.	4,225	39	4,264	2,936	24	2,962 <sup>14</sup>
 <b>External/Removable Media</b> An attack executed from removable media or a peripheral device.	29	3	32	15	0	15
 <b>Impersonation/Spoofing</b> An attack involving replacement of legitimate content/services with a malicious substitute.	93	0	93	272	0	272
 <b>Improper Usage</b> Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	11,669	205	11,874	9,875	248	10,123
 <b>Loss or Theft of Equipment</b> The loss or theft of a computing device or media used by the organization.	1,113	129	1,242	989	82	1,071
 <b>Web</b> An attack executed from a website or web-based application.	2,740	13	2,753	2,722	8	2,730
 <b>Other / Unknown</b> An attack method does not fit into any other vector or cause of attack is unidentified.	9,920	170	10,102	14,014	791	14,805 <sup>15</sup>
 <b>Multiple Vectors</b> An attack that uses two or more of the above vectors in combination.	112	2	114	90	3	93
<b>Total</b>	<b>30,243</b>	<b>564</b>	<b>30,819</b>	<b>31,348</b>	<b>1,161</b>	<b>32,509<sup>16</sup></b>

## 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.<sup>17</sup> The [National Cyber Incident Scoring System \(NCISS\)](#) provides a repeatable and consistent mechanism for estimating the risk of an incident across the Federal enterprise. In the interest of transparency, this report includes a high-level summary of incidents by NCISS priority level for FY 2021 and FY 2020 for comparison, found in Table 5 and visualized in Figure 4.

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% in both fiscal years) were considered “baseline,” meaning that per the [Cybersecurity Incident Severity Schema](#), they are considered “unsubstantiated or inconsequential event[s].”

---

<sup>14</sup> Excludes 2 incidents reported by non-FISMA agencies

<sup>15</sup> Excludes 32 incidents reported by non-FISMA agencies

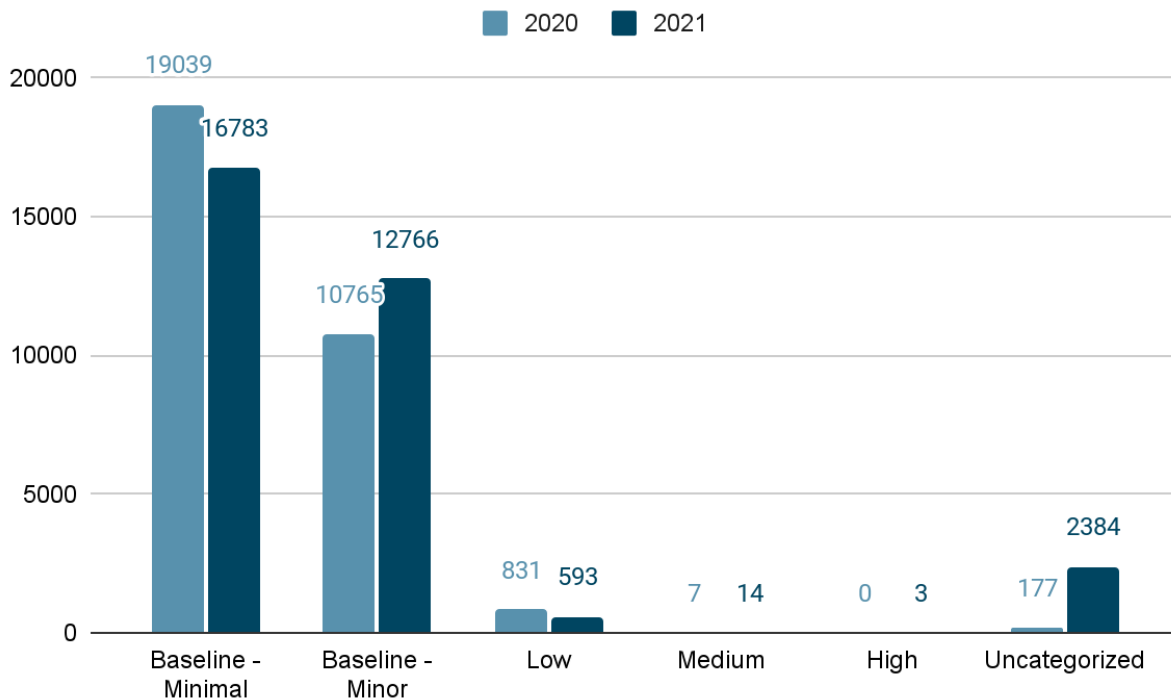
<sup>16</sup> Excludes 34 total incidents reported by non-FISMA agencies

<sup>17</sup> The priority level could change as additional information is discovered during investigation.



**Figure 4 Agency-Reported Incidents by NCISS Score**

---



Source: Incidents reported to CISA in FY 2020 and FY 2021 under M-19-02 and M-20-04 respectively.

---

The increase in **Uncategorized** incidents is a result of three factors:

- RFIs submitted to CISA Central
- Abuse Notifications not assigned an NCISS score
- Valid incidents missing NCISS scores (updated information is being reviewed where available to assign the appropriate NCISS score)

**Table 5 Agency-reported Incidents by NCISS Priority Level**

<b>NCISS Priority Level</b>	<b>FY 2020</b>	<b>FY 2021</b>
<i>Uncategorized</i> Incidents for which insufficient information was collected in order to provide an NCISS priority level.	177	2,384
<b>Baseline – Negligible (White)</b> 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.	19,039	16,783
<b>Baseline – Minor (Blue)</b> Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	10,765	12,766
<b>Low (Green)</b> Unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	831	593
<b>Medium (Yellow)</b> May affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	7	14
<b>High (Orange)</b> Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	0	3
<b>Severe (Red)</b> Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	0	0
<b>Emergency (Black)</b> 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
<b>Total</b>	<b>30,819</b>	<b>32,543<sup>18</sup></b>

Source: Incidents reported to CISA in FY 2020 and FY 2021 under M-19-02 and M-20-04 respectively.

<sup>18</sup> Includes 34 non-FISMA agencies

## Major Incidents

Of the incidents reported by agencies in FY 2021, seven incidents were determined by agencies to meet the threshold for major incidents in accordance with the definition in M-21-02.

In reporting on FY 2021 SAOP FISMA performance measures, CFO Act agencies reported two breaches, as OMB Memorandum M-17-12 defines the term “breach,” to Congress as major incidents during the reporting period. The reporting agencies described those two breaches as potentially affecting 2,831 individuals. Non-CFO Act agencies reported no such breaches.

A summary of major incidents is provided below:

### **SolarWinds**

In December of 2020, the cybersecurity firm FireEye discovered that a SolarWinds product known as Orion was compromised and being leveraged by a threat actor for access to SolarWinds’ customer systems. According to the SolarWinds Chief Executive Officer, hackers breached the company’s network as early as 2019. They inserted malicious code into Orion—a product widely used in both the Federal Government and private sector to monitor network activity and manage devices. The threat actor, the Foreign Intelligence Service of the Russian Federation (SVR), leveraged Orion to breach several Federal agency networks.<sup>19</sup> The initial breach opened a backdoor to agency systems that enabled the SVR to deliver additional malicious code payloads that provided them the capability to move laterally, gathering information and compromising data.

Federal agencies took several steps to coordinate and respond to the SolarWinds incident. This included a unified coordination group with participants from CISA, the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI). Additionally, the National Security Agency (NSA) provided additional support. These agencies provided guidance through various advisories and alerts to assist Federal agencies by informing them about the threat actor’s cyber tools, targets, techniques and capabilities. Additionally, CISA issued an emergency directive to inform and direct agencies to conduct specific actions to take in response to the incident.

The following agencies reported major incidents based on the SolarWinds Orion incident: Department of Commerce, Department of Homeland Security, Department of Justice, National Aeronautics and Space Administration, and Department of the Treasury.

---

<sup>19</sup> <https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/>

## Department of Housing and Urban Development (HUD)

During FY 2021, the Department of Housing and Urban Development (HUD) had a major incident involving a breach of personally identifiable information (PII). Sometime between the dates of May 13, 2021, and June 10, 2021, malware known as QAKBOT was deployed via a successful phishing attack on the hud.gov email account of an Office of General Counsel (OGC) employee. The threat actor used the recipient's compromised .gov email account to send 2,577 emails across HUD, other Federal agencies, and beyond. Seven-hundred internal HUD users were identified as receiving the phishing e-mails. These users' accounts were locked and the HUD Help Desk was able to reimage all 700 systems.

## Department of Commerce

In FY 2021, the Department of Commerce experienced two major incidents, the SolarWinds supply chain compromise and one related to a significant vulnerability in Pulse Connect Secure. Both are believed to have been executed by advanced persistent threat actors.

In April of 2021, a company named Pulse Secure released [a security advisory](#) highlighting a critical remote code execution vulnerability in its Pulse Connect Secure product that affected multiple versions, some of which were in use by Federal agencies. [CISA noted in its advisory](#) that the vulnerability was being exploited by cyber threat actors to gain access to targeted networks.<sup>20</sup>

In addition to supporting the investigation at the Department of Commerce, CISA provided guidance to agencies on remediating the vulnerability and ensuring threat actors had not gained a foothold within Federal systems. Pursuant to requirements under Presidential Policy Directive 41, regular updates were provided to OMB, CISA, and Congress throughout the incident at the Department of Commerce.

## C. Cybersecurity Risk Management

### Integration of Cyber and ERM Programs

FISMA requires Federal agencies to implement information security protections commensurate with their risk environment and to take steps to ensure cybersecurity management is integrated with strategic, operational, and budgetary processes. However, cyber threats are only one of the risks facing the Federal enterprise. Financial, legal, operational, privacy, reputational, and supply chain risks must all be considered.

---

<sup>20</sup> CISA Alert (AA21-110A), "Exploitation of Pulse Connect Secure Vulnerabilities."  
<https://www.cisa.gov/uscert/ncas/alerts/aa21-110a>

Recognizing the importance of addressing the full spectrum of an agency’s internal and external risks, including cybersecurity, OMB Circular A-123 requires Federal agencies to develop enterprise risk management (ERM) programs. Such programs ensure that crosscutting concerns are managed as an interrelated portfolio instead of within silos.

In FY 2017, recognizing the need for agency information security programs to be integrated with ERM programs, the IG FISMA metrics were updated to include specific indicators related to the effectiveness of agency processes in integrating their cyber and ERM programs. At that time, no published guidance highlighted the tools and methodologies that agencies should use to effectively integrate their cyber and ERM programs.

Recognizing the lack of guidance, NIST published [Interagency Report 8286, Integrating Cybersecurity and Enterprise Risk Management](#), in October of 2020. Following the publication’s release, OMB, CISA, and CIGIE worked together to update the FY 2021 IG FISMA metrics, clarifying and streamlining the questions related to integration of cybersecurity and ERM programs. Questions on cybersecurity governance, roles and responsibilities, risk assessment processes, and risk reporting were updated to more clearly delineate agency responsibilities. Furthermore, indicators were added on the use of cybersecurity risk registers as a key tool to manage and communicate cybersecurity risks throughout an organization.

### FY2021 Priority IG Metrics Pilot

Since the FY 2017 FISMA reporting process, IGs have been directed to utilize a mode-based scoring approach to assess agency information security maturity levels. Under this approach, the overall rating for a given domain was equal to the rating most frequently assigned to the metrics within that domain. For example, if a domain included seven metrics, and four of them were assigned a rating of 3, then the domain rating was a 3.<sup>21</sup> The same logic was applied at the function and overall information security program level. While this approach provided an important baseline measure of the maturity of agencies’ information security programs, it did not account for the fact that some metrics are more critical than others.

In the wake of SolarWinds, OMB and CIGIE examined the FISMA reporting process from end to end to identify challenges and pilot solutions for them. In FY 2021 OMB and CIGIE conducted a pilot method of weighting specific IG metrics to drive continued improvements in cybersecurity maturity across the Federal landscape and focus agency efforts. A list of priority metrics and a scoring methodology was developed<sup>22</sup> by analyzing CyberScope data, considering Administration priorities, and identifying the key areas where improvements in capability could lead to demonstrable increases in maturity and observable outcomes.

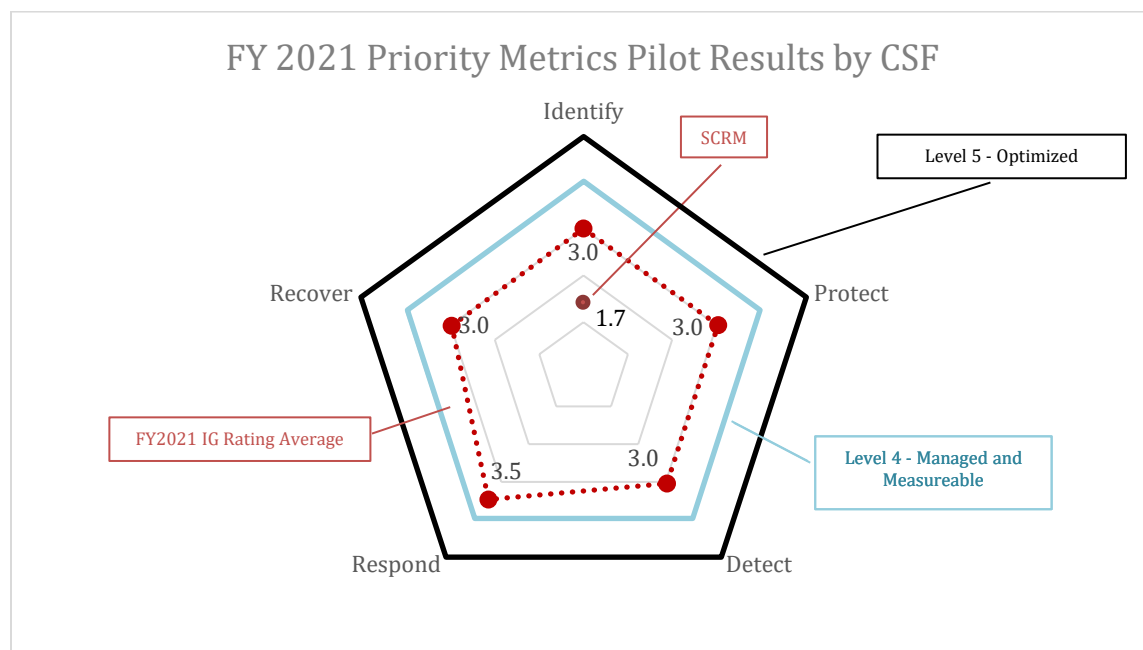
---

<sup>21</sup> See [FY 2021 FISMA IG Metrics \(calculations described in Appendix A\)](#) for IG Rating scale and definitions.

<sup>22</sup> See the proposed weighted metric section in the [FY 2021 FISMA IG Metrics](#).

While the pilot was not used in the overall scoring in FY 2021, Figure 5 below depicts the Government-wide average for IG ratings as developed using the pilot weighting.

**Figure 5 FY 2021 Priority Metrics Pilot Results by CSF**



Source: FY2021 IG Assessment Rating Data

The lessons learned from the pilot led OMB and CIGIE to develop a new framework for assessing agency effectiveness. This framework identified core activities that must be evaluated on an annual basis, while all other metrics can be effectively evaluated on a biennial basis.

As a result of the lessons learned from the pilot, the FY 2022 FISMA Guidance<sup>23</sup> includes a major adjustment to the timing and methodology of the IG assessments, prioritizing metrics for evaluation in the next fiscal year. This shift meets multiple objectives: aligning results to the budget process, reducing reporting burden without compromising the integrity of the required annual evaluation of agency cyber programs, and improving the focus of evaluations on key areas in agency cyber risk management programs. The establishment of the Core IG Metrics process in FY22 will provide a flexible methodology to adjust evaluations and allow agencies to focus cybersecurity efforts on activities that provide greater risk reduction.

<sup>23</sup> [Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements \(whitehouse.gov\)](https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/25/fiscal-year-2021-2022-guidance-on-federal-information-security-and-privacy-management-requirements/)

Further analysis of the Core IG Metrics process will be provided in the next annual FISMA report.

### Supply Chain Risk Management IG Assessment

In FY2021, additional metrics were added to encourage a deeper evaluation of agency Supply Chain Risk Management (SCRM). These metrics establish a baseline, as well as allow for the assessment of SCRM processes and procedures at the agency level. The addition of SCRM metrics highlights the important role SCRM plays in security and allows agencies to identify where additional focus and resources are necessary to improve the overall security posture of their cybersecurity programs. The analysis in Table 6 shows the newly added SCRM questions in FY2021 and the average agency rating for each question.

**Table 6 IG Risk Management Ratings**

IG Metric	FY 2021
12. To what extent does the organization utilize an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services? (The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Sub chap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018), NIST SP 800-53, Rev. 5, PM30, NIST IR 8276)?	1.8
13. To what extent does the organization utilize SCRM policies and procedures to manage SCRM activities at all organizational tiers (The Federal Acquisition Supply Chain Security Act of 2018, NIST 800-53, Rev. 5, SR-1, NIST CSF v1.1, ID.SC-1 and ID.SC-5, NIST IR 8276)?	1.7
14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain requirements. (The Federal Acquisition Supply Chain Security Act of 2018, NIST SP 800-53 REV. 5: SA-4, SR-3, SR-5, SR-6 (as appropriate); NIST SP 800-152; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4, NIST IR 8276). <sup>24</sup>	1.7
15. To what extent does the organization ensure that counterfeit components are detected and prevented from entering the organization’s systems? (800-53 rev 5 SR-11, 11 (1), and 11(2))	1.5
Overall Supply Chain Risk Management Evaluation	1.7

<sup>24</sup> This metric was expanded in scope from previous years to evaluate contracts and cybersecurity oversight of third parties. See [FY2020 IG Metrics \(Question #11\)](#).

Source: Average rating (out of 5, unless otherwise noted) for independently assessed annual IG FISMA Metrics. The rating for FY 2021 reflects the ratings of 85 agencies.

---

The SCRM baselines have been established and, as evident in Figure 5, show that current processes are, on average, performed at a level 1 (Ad Hoc) maturity level. However, the results indicate agencies are applying definition and rigor to their SCRM programs, and are on their way to maturing their SCRM processes. The FASC is leading the effort on an enterprise-wide scale to help the Government as a whole mature in this space.

### Overall Cyber Risk Management Summary

Cybersecurity is not a single action undertaken by an organization; rather, it is a set of strategies that are tailored to the technology and anticipated threats. The changes made to the IG Metrics in FY2021 were designed to describe not only the cyber programs themselves, but also the way these programs are integrated into (and reducing risk for) Federal agencies. Each annual FISMA assessment reflects the maturity of the agency as a whole, gauging the cybersecurity team's impact across all programs.

Cybersecurity continues to remain a top priority in the Biden-Harris Administration. When Federal agencies have effective cybersecurity risk management, they are better able to protect information systems and ensure they can continue their core missions serving the American people. Agencies continue to work with key Administration leadership in OMB and ONCD, as well as with partners at CISA, to develop mature and effective information security risk management programs that are integrated into broader agency programs.



## 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) 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 67 non-CFO Act agencies on FY 2021 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).<sup>25</sup>

---

<sup>25</sup> OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) [hereinafter OMB Circular A-130].

**Table 7 Senior Agency Officials for Privacy (SAOPs) and Privacy Programs**

FY 2021 – SAOP FISMA Performance Measures <sup>26</sup>	CFO	Non-CFO
The head of the agency has designated an SAOP. <sup>27</sup>	100%	97%
Among the agencies that have designated an SAOP:		
The SAOP has the necessary role and responsibilities within the agency for compliance. <sup>28</sup>	100%	98%
The SAOP has the necessary role and responsibilities within the agency for policy making. <sup>29</sup>	100%	98%
The SAOP has the necessary role and responsibilities within the agency for risk management activities. <sup>30</sup>	100%	97%
The agency has developed and maintained a privacy program plan. <sup>31</sup>	100%	85%
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. <sup>32</sup>	100%	89%

## 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

<sup>26</sup> Percentages are rounded to the nearest whole number throughout the SAOP performance measures.

<sup>27</sup> See OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).

<sup>28</sup> See *id.*

<sup>29</sup> See *id.*

<sup>30</sup> See *id.*

<sup>31</sup> 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, *Managing Information as a Strategic Resource*, Appendix I § 4(c)(2), 4(e)(1) (July 28, 2016).

<sup>32</sup> See *id.* at Appendix I § 4(b)(1).

ongoing awareness of their PII holdings and helps to ensure compliance with applicable privacy requirements and to manage privacy risks.

**Table 8 Personally Identifiable Information Inventory**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency maintains an inventory of the agency’s information systems <sup>33</sup> that handle PII. <sup>34</sup>	100%	93%

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 9 Collection, Maintenance, and Use of Social Security Numbers (SSNs)**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
Among the agencies that collect, maintain, or use SSNs, the agency has an inventory of the agency’s collection and use of SSNs. <sup>35</sup>	100%	90%

<sup>33</sup> 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, *Managing Information as a Strategic Resource*, § 10(a)(23) (July 28, 2016).

<sup>34</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(a)(1)(a)(ii), 5(f)(1)(e) (July 28, 2016).

<sup>35</sup> 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.

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.	100%	72%
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.	96%	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%	88%
If the agency has 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. <sup>36</sup>	100%	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.

---

<sup>36</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(f)(1)(f) (July 28, 2016).

**Table 10 Privacy and the NIST Risk Management Framework**

FY 2021 – 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. <sup>37</sup>	100%	95%
Selection, implementation, and assessment of privacy controls. <sup>38</sup>	100%	88%
Authorization of information systems and common controls. <sup>39</sup>	100%	93%
Continuous monitoring of information systems that process PII. <sup>40</sup>	100%	88%
The agency has designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls. <sup>41</sup>	100%	67%
The agency has developed and maintained a written privacy continuous monitoring strategy. <sup>42</sup>	96%	69%
The agency has established and maintained an agency-wide privacy continuous monitoring program. <sup>43</sup>	83%	64%

<sup>37</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 3(a), 3(b)(5) (July 28, 2016).

<sup>38</sup> See *id.*

<sup>39</sup> See *id.*

<sup>40</sup> See *id.*

<sup>41</sup> See *id.* at Appendix I § 4(e)(5); see also *id.* at § 10(a)(14), (26), (66) and (86).

<sup>42</sup> 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, *Managing Information as a Strategic Resource*, Appendix I § 4(d)(9), 4(e)(2) (July 28, 2016).

<sup>43</sup> 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

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 11 Information Systems and Authorizations to Operate**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The number of information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period. <sup>44</sup>	3,483	400
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. <sup>45</sup>	64%	92%
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. <sup>46</sup>	59%	85%

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, *Managing Information as a Strategic Resource*, Appendix I § 4(d)(10)-(11), 4(e)(3) (July 28, 2016).

<sup>44</sup> 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, *Managing Information as a Strategic Resource*, Appendix I § 4(j)(2)(c) (July 28, 2016).

<sup>45</sup> See *id.* at Appendix I § 4(a)(2), 4(e)(7).

<sup>46</sup> 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, *Managing Information as a Strategic Resource*, Appendix I § 4(c)(9), (e)(8) (July 28, 2016).

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. <sup>47</sup>	64%	84%
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. <sup>48</sup>	59%	89%

## 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 12 Information Technology Systems and Investments**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency has a policy that includes explicit criteria for analyzing privacy risks when considering IT investments. <sup>49</sup>	83%	64%

<sup>47</sup> See *id.* at Appendix I § 4(e)(3).

<sup>48</sup> See *id.* at Appendix I § 4(e)(9).

<sup>49</sup> 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. <sup>50</sup>	71%	69%
The agency maintains an inventory of the agency’s information technology systems that handle PII.	100%	96%

### 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 13 Privacy Impact Assessments**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
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.	4,197	779
The number of 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	3,602	641

<sup>50</sup> See *id.* at § 5(a)(3)(e)(ii).



under the E-Government Act of 2002 that are covered by an up-to-date PIA. <sup>51</sup>		
Among the agencies that have a written policy for PIAs, the written policy for PIAs includes: <sup>52</sup>		
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%	90%
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%	94%
The agency has a process or procedure for: <sup>53</sup>		
Assessing the quality and thoroughness of each PIA.	100%	78%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	100%	76%
Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated.	96%	76%
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%	78%

## 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

<sup>51</sup> 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, *Managing Information as a Strategic Resource*, Appendix II § 5(e) (July 28, 2016).

<sup>52</sup> See *id.* at Appendix II § 5(e) (July 28, 2016).

<sup>53</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix II § 5(e) (July 28, 2016).

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 14 Workforce Management**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency ensures that the agency’s privacy workforce has the appropriate knowledge and skill. <sup>54</sup>	96%	96%
The agency has assessed its hiring, training, and professional development needs with respect to privacy during the reporting period. <sup>55</sup>	92%	88%
The agency has developed a workforce planning process to ensure that it accounts for privacy workforce needs. <sup>56</sup>	83%	72%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions. <sup>57</sup>	75%	70%

**Table 15 Training and Accountability**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency provides foundational privacy training to its Federal employees (including managers and senior executives). <sup>58</sup>	100%	97%
The agency provides role-based privacy training to Federal employees with assigned privacy roles and responsibilities, including managers, before authorizing their access to Federal information or information systems. <sup>59</sup>	79%	60%

<sup>54</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(c)(2) (July 28, 2016).

<sup>55</sup> See *id.* at § 5(c)(6).

<sup>56</sup> See *id.* at § 5(c)(1).

<sup>57</sup> See *id.*

<sup>58</sup> See *id.* at Appendix I § 4(h)(4); see also *id.* at Appendix I § 4(h)(1).

<sup>59</sup> See *id.* at Appendix I § 4(h)(5); see also *id.* at Appendix I § 4(h)(1).

The agency has ensured measures are in place to test the knowledge level of information system users in conjunction with privacy training. <sup>60</sup>	96%	81%
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. <sup>61</sup>	100%	99%
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. <sup>62</sup>	100%	94%

**Table 16 Contractors and Third Parties**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors. <sup>63</sup>	100%	90%
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. <sup>64</sup>	100%	99%
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. <sup>65</sup>	100%	95%

<sup>60</sup> See *id.* at Appendix I § 4(h)(4).

<sup>61</sup> See *id.* at Appendix I § 4(h)(6).

<sup>62</sup> See *id.* at Appendix I § 4(h)(7).

<sup>63</sup> See *id.* at Appendix I § 4(h)(1), (4)-(5).

<sup>64</sup> See *id.* at Appendix I § 4(h)(6).

<sup>65</sup> See *id.* at Appendix I § 4(h)(7).

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: <sup>66</sup>		
Processes do not exist.	0%	1%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	13%	28%
Processes are fully documented and implemented and cover all relevant aspects.	17%	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.	71%	43%
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: <sup>67</sup>		
Processes do not exist.	0%	0%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	4%	25%
Processes are fully documented and implemented and cover all relevant aspects.	25%	24%
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.	71%	51%

## 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

<sup>66</sup> See *id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).

<sup>67</sup> See *id.* at Appendix I § 4(j)(2)(a).

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.<sup>68</sup>

**Table 17 Breach Response**

<b>FY 2021 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
Among the agencies that have a breach response plan, the breach response plan includes the agency’s policies and procedures for: <sup>69</sup>		
Reporting a breach	100%	100%
Investigating a breach	100%	98%
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. <sup>70</sup>	96%	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. <sup>71</sup>	100%	94%
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. <sup>72</sup>	63%	63%
The number of breaches, as OMB Memorandum M-17-12 defines the term “breach,” that were reported within agencies during the reporting period. <sup>73</sup>	16,628	1,286

<sup>68</sup> See OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).

<sup>69</sup> See *id.* at § VII, XI.

<sup>70</sup> See *id.* at § X.B, XI.

<sup>71</sup> See *id.* at § VII.A, XI.

<sup>72</sup> See *id.* at § X.A, XI.

<sup>73</sup> See *id.* at § III.C, XI.

The number of breaches, as OMB Memorandum M-17-12 defines the term “breach,” that agencies reported to DHS Cybersecurity and Infrastructure Security Agency (CISA) during the reporting period. <sup>74</sup>	12,263	75
---	--------	----

---

<sup>74</sup> 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 to by attack vector. The descriptions below provide an overview of the sections included in each agency performance summary.

## CIO Self-Assessments and CIO Ratings

The CIO self-assessment is a written narrative which provides each agency with an opportunity to offer insight into the successes or challenges from the past year, and, in some cases, articulate the agency’s future priorities.

CIO ratings are based on the RMA process described in OMB M-17-25 which leverages the [FY 2021 FISMA CIO Metrics](#) in domains that correspond with the NIST CSF functions:

- **Identify** (Asset Management; System Authorization);
- **Protect** (Remote Access Protection; Credentialing and Authorization; Configuration and Vulnerability Management; HVA Protection);
- **Detect** (Intrusion Detection and Prevention; Exfiltration and Enhanced Defenses); and
- **Respond and Recover**<sup>75</sup>.

Agency ratings fall within the following schema:

- **High Risk:** Key, fundamental cybersecurity policies, processes, and tools are either not in place or not deployed sufficiently.
- **At Risk:** Some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain.
- **Managing Risk:** The agency institutes required cybersecurity policies, procedures, and tools and actively manages their cybersecurity risks.

---

<sup>75</sup> Revisions to FY 2018 CIO metrics reduced the number of metrics in the Respond and Recover framework functions. Due to this reduction in number and the interconnectedness, these post-incident functions have been combined into a single area of assessment for the purposes of the RMAs.

## 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 2021 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  
FASC - Federal Acquisition Security Council  
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

NSSC - National Security Coordination Council  
NSS - National Security Systems  
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