Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2020

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, § 3553, 44 U.S.C. § 3553. This report also incorporates OMB's analysis of agency application of the intrusion detection and prevention capabilities, as required by Section 226(c)(1)B) of the Cybersecurity Act of 2015, Pub. L. No. 114-113, and incorporates agency reporting on complying with privacy requirements and managing privacy risks. OMB obtained information from the Department of Homeland Security (DHS), 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 2020 data reported by agencies to OMB and DHS.

Table of Contents

Executive Summary: The State of Federal Cybersecurity

Cybersecurity remains a significant challenge in the Federal Information Technology (IT) landscape. In December 2020, it was discovered that a sophisticated supply chain attack was used to gain access to a large number of information systems across several Federal Government agencies and U.S.-based companies. Commonly associated with the SolarWinds software that was among those exploited, this protracted attack was perpetrated by well-resourced actors spanning several months and is one of many reasons that the President has made cybersecurity one of the top priorities of his Administration. These events serve as a reminder that the Federal Government must continually invest in defensive capabilities in order to reduce the impact of cybersecurity incidents on our Nation.

Agencies reported 30,819 cybersecurity incidents in fiscal year (FY) 2020, an 8% increase over the 28,581 incidents that agencies reported in FY 2019. This trend highlights the ever-increasing threats within the digital landscape and the need for the Federal Government to take action to reduce the impact of cybersecurity incidents. With respect to this same time period, agencies reported six major incidents to the Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency (CISA), and Congress. The incidents covered in this document were reported to CISA during FY 2020, which spans October 1, 2019 to September 30, 2020. Incidents related to the compromise of SolarWinds software are not directly covered in this report because they were first reported in December 2020, after the FY 2020 reporting period. Those incidents, for which facts continue to evolve, will be more directly addressed in the FY 2021 FISMA report.

FY 2020 Report Key Takeaways:

30,819 incidents were reported in FY 2020 (8% increase over previous year), six of which were reported as major incidents.

Agencies continue to show improvements in available cyber hygiene measures; however, more work is necessary.

Agencies were able to quickly and securely respond to the shift to telework during the COVID-19 pandemic.

The coronavirus disease 2019 (COVID-19) pandemic National emergency was also a significant factor in information security during FY 2020. This report highlights successful agency efforts during FY 2020 to rapidly transition the Federal enterprise to a telework posture during the ongoing pandemic.

Due to the consistency in reporting metrics between FY 2017 and FY 2020, this report is able to demonstrate the long-

term improvement of cybersecurity hygiene across the Federal Government. This report also highlights Government-wide programs and initiatives as well as agencies' progress to enhance Federal cybersecurity over the past year; however, the work of cybersecurity is never done, as adversaries constantly evolve and so must the defenders. Included in this report are a series of findings and actions for the Administration derived from data collected from departments and agencies.

In addition to the focus on cybersecurity, this report offers insight into agencies' privacy performance through their responses to Senior Agency Official for Privacy (SAOP) metrics. While privacy and cybersecurity are independent and separate disciplines, coordination between them is critical to agencies' efforts to protect the information entrusted to them.

Section I: Federal Cybersecurity Activities

A. Roles and Responsibilities

FISMA identifies the agency head as the responsible official for their respective organization's cybersecurity posture. Agencies are responsible for allocating the necessary people, processes, and technology to protect Federal data. Each agency head is responsible for delegating this authority to the Chief Information Officer (CIO), including the authority to designate a Senior Agency Information Security Official or Chief Information Security Officer (CISO).

Enhancing Federal cybersecurity is a collective effort that requires participation from all personnel across the Federal enterprise. The following section provides a brief overview of agency key roles and responsibilities in strengthening Federal cybersecurity in accordance with statute, policy, and the agency's mission.

Office of Management and Budget (OMB): OMB is statutorily responsible for overseeing Federal agencies' information security and privacy practices, as well as for developing and directing implementation of policies and guidelines which support and sustain those practices. Within OMB, the Office of E-Government and Information Technology, also known as the Office of the Federal Chief Information Officer (OFCIO), implements OMB's information security responsibilities. The Federal Chief Information Security Officer engages with Federal agency leadership to address information security priorities. OFCIO also collaborates with partners across the Government to develop cybersecurity policies, conduct data-driven oversight of agency cybersecurity programs, and coordinate the Federal response to cyber incidents. OMB's Office of Information and Regulatory Affairs (OIRA) is responsible for developing Federal privacy policy, overseeing implementation of privacy policy by Federal agencies, and assisting Federal agencies on privacy matters.

National Security Council (NSC): NSC is the Executive Office of the President (EOP) component responsible for coordinating policy initiatives with the President's senior advisors, cabinet officials, and military and intelligence community leaders. The President has appointed a Deputy National Security Advisor for Cyber and Emerging Technology who works on cybersecurity issues and advises the President on National security and foreign policy matters related to cybersecurity. NSC and OMB closely coordinate and collaborate with Federal agencies to implement the Administration's cybersecurity priorities.

Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA): CISA is the operational lead for Federal civilian executive branch (FCEB) cybersecurity and has the authority to coordinate cybersecurity efforts across all FCEB

agencies, issue Binding Operational Directives (BODs) and Emergency Directives (EDs),[1] in coordination with OMB. BODs and EDs detail actions that agencies must take to improve their cybersecurity and to provide operational and technical assistance to agencies. To achieve these objectives, CISA operates the Federal information security incident center. Under FISMA and other authorities, CISA provides common security capabilities for agencies through the National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) program. Additionally, CISA provides Federal asset response activities through National Cybersecurity and Communications Integration Center (NCCIC) in accordance with Presidential Policy Directive-41, United States Cyber Incident Coordination (PPD-41). Finally, CISA plays a key role in facilitating information sharing across the Federal, state, local, tribal, and territorial governments, and the private sector.

General Services Administration (GSA): GSA provides management and administrative support to the entire Federal Government and establishes acquisition vehicles for agencies to purchase cybersecurity products and services. Additionally, GSA provides administrative assistance for the Chief Information Officers Council (CIOC), Chief Information Security Officers Council (CISOC), and Federal Privacy Council (FPC). GSA also operates the Federal Risk and Authorization Management Program (FedRAMP), which promotes the use of secure cloud-based services in Government.

National Institute of Standards and Technology (NIST): NIST, a component of the Department of Commerce, develops standards and guidelines for Federal information systems, in coordination with OMB and other Federal agencies. Among other roles, NIST creates Federal Information Processing Standards (FIPS) and releases Special Publications (SPs) that provide management, operational, and technical security guidelines on a broad range of topics, including intrusion detection, incident handling, supply chain risk management, and definition of strong authentication protocols. NIST develops, updates, and publishes a series of standards and frameworks, including the Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF). Recently, NIST has integrated privacy into some of its information security documents.

Federal Bureau of Investigations (FBI): The FBI, a component of the Department of Justice, leads Federal investigations of cybersecurity intrusions and attacks carried out against public and private targets by criminals, overseas adversaries, and terrorists. The FBI's capabilities and resources for handling cybersecurity-related issues include a Cyber Division, globally deployable Cyber Action Teams, cybersecurity organizations, and partnerships with Federal, state, and local law enforcement.

[1] 44 U.S.C. § 3553(h)(1)–(2)

The Intelligence Community (IC): Led by the Office of the Director of National Intelligence (ODNI), the IC provides vital intelligence to the Federal Government. An essential component of cybersecurity is obtaining and analyzing information on the threats and malicious actors targeting both public and private infrastructure.

Office of the National Cyber Director (ONCD): The National Defense Authorization Act for FY 2021 establishes this office within the Executive Office of the President (EOP), headed by a National Cyber Director. The Biden Administration is committed to standing up this office for success and will ensure its establishment is informed by lessons learned from the recent supply chain security event.

B. Programs and Policy Areas

Continuous Diagnostics and Mitigation (CDM)

Prior to the establishment of the Continuous Diagnostics and Mitigation (CDM) program by DHS, Federal agencies inconsistently implemented Information Security Continuous Monitoring (ISCM) policies. The CDM program provides a dynamic approach for baselining ISCM efforts: DHS's CDM program provides Federal agencies with the tools, integration services, and dashboards necessary for identifying cybersecurity risks on a continuous basis. This near real-time monitoring enhances agencies' ability to prioritize cybersecurity risks, enabling cybersecurity personnel to mitigate the most significant problems first. The CDM program also provides CISA with a Federal enterprise view of the cyber threat landscape through the Federal CDM Dashboard that 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 FISMA reporting.

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 acquisition vehicles. Additionally, M-21-02 requires that CISA fund the initial procurement of the CDM tool, as well as the first year of operations and maintenance (e.g., licensing) costs. Large Federal agencies are required to fund long-term operations and maintenance of their CDM-related tools. 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 PMO will cover CDM license costs for certain non-CFO Act agencies. The memorandum also requires agencies to take various steps to improve the quality of their data exchanged with the Federal CDM dashboard.

National Cybersecurity Protection System (NCPS)

NCPS, of which the EINSTEIN system is a component, provides a suite of tools to enhance the boundary awareness and security of Federal agencies. The most recent of these capabilities 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 Federal civilian executive branch traffic enabling the deployment of new and advanced protections by CISA. Table 1 demonstrates the implementation status as of September 30, 2020.

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

EINSTEIN Capability	● Complete	◑ In Progress	◌ Deferred[2]	○ Not Implemented
E1/E2	80	0	0	28
CFO	23	0	0	0
Non-CFO	57	0	0	28
E3A Email	81	5	3	18
CFO	23	0	0	0
Non-CFO	58	5	3	18
E3A DNS	86	1	2	15
CFO	23	0	0	0
Non-CFO	63	1	2	15

Coordinated Vulnerability Disclosure (CVD)

Coordinated Vulnerability Disclosure (CVD) enables agencies to improve their information security programs by harnessing cybersecurity talent from outside the Government. In FY 2020, OMB in coordination with the CISA issued OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation* and CISA BOD-20-01, *Develop and Publish a Vulnerability Disclosure Policy* requiring agencies to solicit and review vulnerability findings from the general public. CVD is among the most effective methods for obtaining new insights regarding security vulnerability information and can provide high return on

[2] 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.

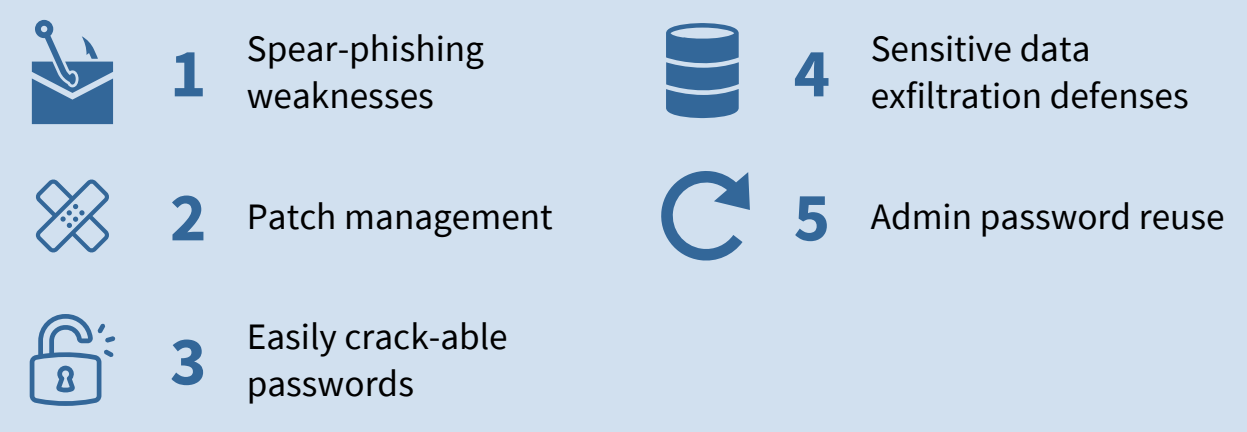
investment. CVD also provides protection for those who uncover these vulnerabilities by defining good-faith security research. In this effort to improve our cyber defenses and Government transparency, all Federal agencies shall develop implementation plans providing timelines and milestones for Vulnerability Disclosure Policy (VDP) to cover all Federal information systems by May 2, 2021.

High Value Assets (HVAs)

The High Value Asset (HVA) Program is designed to increase the resiliency of the Federal Government's critical information systems to prevent cybersecurity-related breaches, mitigate cyber risks, and improve enterprise risk management. The HVA Program provides cybersecurity services aimed at identifying vulnerabilities and enhancing the cybersecurity posture of the Federal Government's HVA systems.

In FY 2020, CISA conducted 61 HVA assessments, resulting in 348 findings (compared to 71 assessments with 448 findings in FY 2019). These findings consisted of 261 System Architecture Review (SAR) findings and 87 Risk and Vulnerability Assessment (RVA) findings. Due to COVID-19 restrictions and the on-site requirements to conduct RVA assessments, the last HVA RVA for FY20 was conducted in March 2020. These assessments revealed that the Federal Government continues to face challenges in mitigating basic security vulnerabilities. The most common security deficiencies identified across the HVA landscape are identified in Figure 1.

Figure 1 Top 5 RVA findings in FY 2020



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.

Leading up to the release of the new policy, the Small Business Administration (SBA) and the Department of Energy (DOE) worked with OMB and CISA to pilot selected solutions. The success of these pilots demonstrates that solutions using current technologies can allow this program to continue to make progress on goals outlined a decade ago.

In July 2020, following the public comment period, CISA, OMB, and the CISO Council released updated guidance to assist agencies in the proposal and implementation of additional pilot efforts. These entities are actively engaged with agencies on additional pilots that will soon add to the use cases available for agencies to leverage cloud-based solutions.

Supply Chain Risk Management

With the passage of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act, agencies are required to assess the risks to their respective information and communications technology supply chains. In addition to agency Supply Chain Risk Management (SCRM) programs, enterprise-wide risk is being addressed through the Federal Acquisition Security Council (FASC). The FASC will make recommendations on potential exclusion and removal orders to the Secretaries of Defense and Homeland Security, as well as the Director of National Intelligence, to address risk to each of their enterprises. These critical steps help agencies safeguard information and communication technology from emerging threats and support the need to establish standards for the acquisition community around SCRM.

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 Operational Directives (BODs) and Emergency Directives (EDs), outlining activities where Federal agencies are required to comply. BODs address agency implementation of OMB policies, principles, standards, and guidelines. EDs address known or reasonably suspected information security threats, vulnerabilities, and incidents that represent a substantial threat to agencies.

CISA leads DHS efforts to develop, communicate, and manage actions and critical activities related to all directives, in close coordination with OMB. DHS issued one BOD and three EDs in FY 2020:

- **BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy:** This directive requires each agency to develop and publish a VDP and maintain supporting handling procedures, issued in support of M-20-32. As of December 1, 2020, four agencies had published a VDP on their main .gov domain webpage.
- **ED 20-02: Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday:** On January 14, 2020, Microsoft released a software patch to mitigate significant vulnerabilities in supported Windows operating systems. Among the vulnerabilities

patched were weaknesses in how Elliptic Curve Cryptography (ECC) validates certificates and connection requests are handled in the Remote Desktop Protocol (RDP) server and client. CISA determined that these vulnerabilities posed an unacceptable risk to the Federal enterprise and required agencies to patch all applicable end points. As of December 30, 2020, 99% of reported Windows Server operating systems have been mitigated, and 90 agencies completed the Directive requirements.

- **ED 20-03: Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday:** On July 14, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1350). A remote code execution vulnerability exists in how Windows Server is configured to run the Domain Name System (DNS) Server role. If exploited, the vulnerability could have allowed an attacker to run arbitrary code in the context of the Local System Account. CISA determined that this vulnerability posed an unacceptable significant risk to the Federal enterprise and required agencies to update all applicable endpoints. As of December 30, 2020, 97% of reported Windows Server operating systems running the DNS role have been mitigated, and 75 agencies completed the Directive requirements.
- **ED 20-04: Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday:** On August 11, 2020, Microsoft released a software update to mitigate a critical vulnerability in Windows Server operating systems (CVE-2020-1472). The vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory, could have allowed an unauthenticated attacker with network access to a domain controller to completely compromise all Active Directory identity services. CISA determined that this vulnerability posed an unacceptable significant risk to the Federal enterprise and required agencies to update all applicable endpoints. As of December 30, 2020, 96% of reported Windows Server operating systems have been mitigated, and 96 agencies completed the Directive requirements.

Section II: Federal Cybersecurity Reporting and Analysis

OMB must leverage data to support policy making and program operations in order to improve their effectiveness. In the interest of transparency, OMB publishes a portion of the collected data to the public in order to support these processes. This section of the report includes several findings and identified actions based on this data.

A. Improvements in Cybersecurity Hygiene

Cybersecurity Cross-Agency Priority (CAP) Goal Performance

The Government Performance and Results Modernization Act (GPRAMA) of 2010 provides a mechanism for accelerating progress in priority areas in which implementation requires active collaboration between OMB and Federal agencies. As part of this process, OMB establishes Cross Agency Priority (CAP) Goals which include performance targets, and agencies report progress toward these goals as part of the FY 2020 FISMA CIO Metrics collection process outlined in OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements* (now superseded by M-21-02).

A summary of the Federal Government's overall performance on these cybersecurity metrics from FY 2017 to FY 2020 can be found below in Table 2, based on responses from 96 agencies in FY 2020. The Federal Government has made significant progress on these metrics, indicating the continuing improvement of information security hygiene. As the Administration sets its cybersecurity agenda, OMB will select and/or create new metrics with consideration to the CAP Goal process as a potential tool to drive priorities.

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. Where the CAP Goal targets focus on a handful of metrics, the RMA covers a larger set of information security controls and capabilities in alignment with the NIST CSF.

Table 2 FY 2017 - FY 2020 CAP Goal Metric Summary

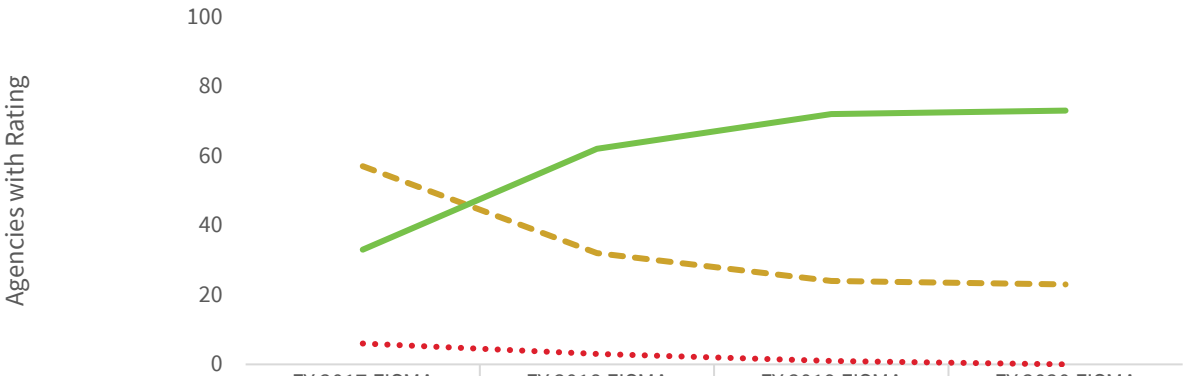
CAP Goal Metric	Target	Number of Agencies Meeting Target				Average Implementation*			
		FY 2017	FY 2018	FY 2019	FY 2020	FY 2017	FY 2018	FY 2019	FY 2020
Manage Asset Security									
Hardware Asset Management	95%	58	71	73	75	67%	64%	70%	85%
Software Asset Management	95%	53	56	70	78	69%	58%	75%	85%
Authorization Management**	100%	51	79	81	77	84%	91%	94%	94%
Mobile Asset Management	95%	N/A	78	89	90	N/A	96%	99%	99%
Limit Personnel Access									
Privileged Network Access Management	100%	46	56	58	61	93%	94%	96%	96%
High Value Asset System Access Management**	90%	N/A	58	66	71	N/A	70%	75%	81%
Automated Access Management	95%	N/A	63	67	72	N/A	63%	88%	92%
Protect Networks and Data									
Intrusion Detection and Prevention	4 of 6	N/A	45	60	75	N/A	N/A	N/A	N/A
Exfiltration and Enhanced Defenses	90%	N/A	66†	79	79	N/A	N/A	N/A	N/A
Data Protection**	4 of 6	N/A	67	75	81	N/A	N/A	N/A	N/A

Source: CAP Goal Metrics FY 2020 FISMA CIO Metrics (calculations described in Appendix A) representing 96 agencies in FY 2020 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 considered meeting related metrics, and are not considered in weighted average.
† In FY 2018 the vast majority of agencies (93, including all 23 civilian CFO Act agencies) had met 3 of the 4 original targets set in the Exfiltration and Enhanced Defenses CAP goal, and OMB considered this target to be achieved. As a result, the target was shifted to the remaining metric concerning exfiltration detection (FISMA CIO Metric 3.8). This figure represents the number of agencies meeting the new target in FY 2018.

In FY 2017 six agencies received a rating of "High Risk"[3] (the poorest rating), with 33 agencies receiving the rating of "Managing Risk" (the best rating). As of FY 2020 reporting, no agencies received a rating of "High Risk," and 73 agencies received a rating of "Managing Risk." A summary of the RMA ratings from FY 2017 to FY 2020 can be found below in Figure 2, based on responses from 96 agencies in FY 2020.

While the RMA served as a helpful mechanism in driving progress and accountability in these measures, the process must be revised now that the majority of agencies are meeting targets. OMB will continue to develop improvements to its cybersecurity scorecard processes in alignment with Administration priorities, agency risk profiles, and the ever-evolving threat environment, applying lessons learned from the RMA process.

Figure 2 Agency Risk Management Assessment (RMA) Ratings



	FY 2017 FISMA Report	FY 2018 FISMA Report	FY 2019 FISMA Report	FY 2020 FISMA Report
High Risk	6	3	1	0
At Risk	57	32	24	23
Managing Risk	33	62	72	73

Source: RMA ratings based on FY 2020 FISMA CIO Metrics representing 96 agencies in FY 2020 and previous annual FISMA reports.

Independent Assessments[4]

FISMA requires each agency Inspector General (IG), (or independent assessors),[5] to conduct an annual independent evaluation to determine the effectiveness of the information security

[3] For a complete description of the RMA ratings, see Appendix I.
[4] 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.
[5] 44 USC § 3555(b)(2) requires that for agencies without an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

program and practices of their respective agency. Each year these independent assessors respond to FY 2020 IG FISMA Metrics which are developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) in coordination with OMB and CISA. Each metric and the functions of the NIST CSF are provided a rating on a maturity model with five levels.[6]

Pursuant to OMB M-20-04 and IG Reporting 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 in evaluating the maturity of their agencies' cybersecurity programs considering 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 rely on the performance metrics to determine the effectiveness of their agencies' cybersecurity programs. Table 3 shows the number (and percentage) of agencies determined as having an effective information security program from FY 2017 to FY 2020. The percentage of agency information security programs which were evaluated as effective improved from 48% to 60%.

Table 3 IG Information Security Effectiveness Ratings

IG Metric	FY2017	FY2018	FY2019	FY2020
Number of agency information security programs rated as overall "Effective" by their independent assessment, per OMB M-20-04[7]	39 (48%)	43 (51%)	45 (54%)	52 (60%)

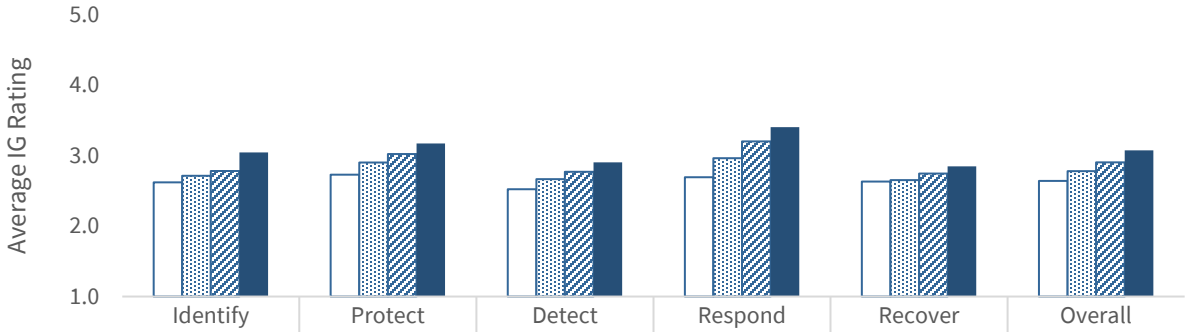
Source: Independent assessments of information security programs from FY 2020 IG FISMA Metrics (or applicable year) representing 86 agencies in FY 2020

Figure 3 depicts the IG CSF ratings from FY 2017 to FY 2020, across 86 agencies (in FY 2020) weighted equally. The average rating for each CSF function improved from 2.6 (above the threshold for *Defined* on the maturity scale) to 3.1 (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.

[6] For a complete description of IG ratings, see Appendix I.

[7] Or the respective OMB memoranda applicable at the time of the evaluation.

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



	Identify	Protect	Detect	Respond	Recover	Overall
FY 2017	2.6	2.7	2.5	2.7	2.6	2.6
FY 2018	2.7	2.9	2.7	3.0	2.7	2.8
FY 2019	2.8	3.0	2.8	3.2	2.7	2.9
FY 2020	3.0	3.2	2.9	3.4	2.8	3.1

Source: Unweighted average rating (out of 5) for each NIST CSF Function based on independent assessments from FY 2020 IG FISMA Metrics (or applicable year) representing 86 agencies in FY 2020

B. Response to the COVID-19 Emergency

Shift to Telework

In March 2020, as state, county, and city governments began to impose various levels of "stay-at-home" orders to reduce the spread of the virus, agency heads using their authorities and following OMB and Office of Personnel Management (OPM) guidance provided much of their workforce with significant telework flexibilities. This dramatic increase in the number of remotely working employees required rapid acquisition of hardware and software, expansion of Virtual Private Networks (VPNs), enhancement of infrastructure, modification of telecommunications contracts, and reconfiguration of networks. Whether or not agencies had made contingency plans for this specific type of scenario, the Federal enterprise was able to quickly and securely transition to mass telework posture and resume the work necessary to fulfill their missions.

Agency Cybersecurity Performance Summaries that described in Appendix I of this report include a written CIO self-assessment. The prompt for this year's report was: "*Provide a narrative assessment of the cybersecurity risks to the agency and the steps the agency has undertaken in FY 2020 to mitigate them, to include the mitigation of risks during the expansion of telework under the COVID-19 national emergency*." A broad review of these narratives indicates that agencies were able to quickly implement the necessary IT infrastructure to support this shift, and these narratives include examples of how agencies were able to make risk-based decisions and maintain continuity of operations.

OMB reduced reporting burden during this time by cancelling the April 2020 FISMA CIO metrics collection. Additional reporting flexibilities were provided to IGs so they could conduct portions of their annual independent assessments that needed to be performed in-person, and were encouraged to conduct assessments remotely to the greatest extent practicable.

Table 4 below, which includes the Government-wide average IG rating (out of 5, unless otherwise specified) for 8 metrics from FY 2017 to FY 2020, demonstrates how over time agencies have improved security of remote access (31) and how agency contingency planning has improved (60-66), providing context for the government's ability to respond to this shift to telework in a timely manner.

Table 4 IG Remote Access and Contingency Planning Ratings

IG Metric	FY2017	FY2018	FY2019	FY2020
31. To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections?	3.0	3.2	3.2	3.3
60. To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority?	2.7	2.6	2.9	3.1
61. To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate?	2.5	2.7	2.7	2.8
62. To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts? (out of 3)	2.2	2.2	2.3	2.4
63. To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	2.5	2.7	2.9	3.0
64. To what extent does the organization perform tests/exercises of its information system contingency planning processes	2.6	2.7	2.7	2.8
65. To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate? (out of 3)	2.5	2.6	2.6	2.7
66. To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions?	2.7	2.7	2.8	3.0

Source: Unweighted average rating (out of 5, unless otherwise noted) for independently assessed FY 2020 IG FISMA Metrics (or applicable year) representing 86 agencies in FY 2020

System Authorizations and Cloud

Federal agencies stood up new systems to support mass telework posture, and in many cases these were hosted with cloud service providers. Agencies reported a 6% increase in the total number of FISMA systems and a 26% increase in the total number of cloud services in FY 2020,

relative to the numbers of these items reported FY 2019. The vast majority of these new systems received an Authority to Operate (ATO) by the end of the fiscal year, as the proportion of Moderate and High Impact Systems [8] with ATOs remained approximately 94% across the enterprise.

The COVID-19 pandemic highlighted known issues with the ATO process, as agencies were placed in the difficult position of having to rapidly implement necessary systems. Because the ATO process remains lengthy, costly, and primarily focused on compliance rather than risk, OMB and CISA continue to evaluate policy and program options for ATOs. OMB and the FedRAMP PMO continue to innovate the FedRAMP authorization process so that it leans on data automation, controls inheritance through profiles of well-established CSPs, and focuses on risk management, which will enable agencies use cloud and innovative technologies to safely enable their missions.

Table 5 IG System Authorization Ratings

IG Metric	FY2017	FY2018	FY2019	FY2020
1. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections? (out of 3 in 2017, out of 5 in 2018-2020)	2.4	3.0	3.0	3.2
11. To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services?	2.6	2.7	2.8	3.0
49. How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls?	2.6	2.8	2.8	3.0

Source: Unweighted average rating (out of 5, unless otherwise noted) for independently assessed FY 2020 IG FISMA Metrics (or applicable year) representing 86 agencies in FY 2020

[8] As described in Federal Information Processing Standard Publication 199 (FIPPS-199), Standards for Security Categorization of Federal Information and Information Systems

C. FY 2020 Information Security Incidents

M-20-04 requires agencies to report information security incidents to CISA in accordance with CISA's Incident Notification Guidelines. This includes events that have been under investigation for 72 hours without successful determination of the event's root cause or nature (i.e., malicious, suspicious, or benign). As required in FISMA, this report provides summary information on the number of cybersecurity incidents that occurred across the Federal Government.

Incidents by Attack Vector[9]

As part of reporting requirements, agencies must classify incidents by the method of attack, known as attack vector.[10] This incident data provides an indication of the types of threats agencies face every day and the persistence of those incidents. This report includes the number of incidents of each type across the Federal enterprise to better understand and oversee the threat landscape. Additionally, the Agency Cybersecurity Performance Summaries that appear in Appendix I include a summary at the agency level.

Table 6 highlights 30,819 incidents reported by Federal agencies and validated with CISA across nine attack vector categories, representing an 8% increase from FY 2019 when agencies reported 28,581 incidents. The growing number of incidents continue to indicate that cybersecurity requires constant vigilance.

Improper Usage remains the most common vector with 11,874 incidents (nearly 39%). The prevalence of this vector indicates that agencies have processes or capabilities that detect when a security policy is being violated, but lack automated enforcement or prevention mechanisms. The "Other/Unknown" vector was the second most common vector with 10,102 incidents (about 33%). The prevalence of this attack vector suggests additional steps should be taken to ensure agencies appropriately categorize the vector of incidents during reporting. OMB and CISA will continue to work with agencies to improve the quality of incident reporting data to ensure the vectors of incidents are appropriately categorized.

[9] 44 USC § 3553(c)(1).

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

Table 6 Agency-reported Incidents by Attack Vector

Attack Vector	FY 2019 CFO*	FY 2019 Non-CFO*	FY 2019 Gov-wide	FY 2020 CFO	FY 2020 Non-CFO	FY 2020 Gov-wide
Attrition An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	327	5	332	342	3	345
E-mail/Phishing An attack executed via an email message or attachment.	4,102	286	4,388	4,225	39	4,264
External/Removable Media An attack executed from removable media or a peripheral device.	46	1	47	29	3	32
Impersonation/Spoofing An attack involving replacement of legitimate content/services with a malicious substitute.	35	0	35	93	0	93
Improper Usage Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	12,280	227	12,507	11,669	205	11,874
Loss or Theft of Equipment The loss or theft of a computing device or media used by the organization.	1,685	200	1,885	1,113	129	1,242
Web An attack executed from a website or web-based application.	1,933	49	1,982	2,740	13	2,753
Other / Unknown An attack method does not fit into any other vector or cause of attack is unidentified.	7,006	234	7,240	9,920	170	10,102
Multiple Attack Vectors An attack that uses two or more of the above vectors in combination.	158	7	165	112	2	114
Total	**27,572**	**1,009**	**28,581**	**30,243**	**564**	**30,819**

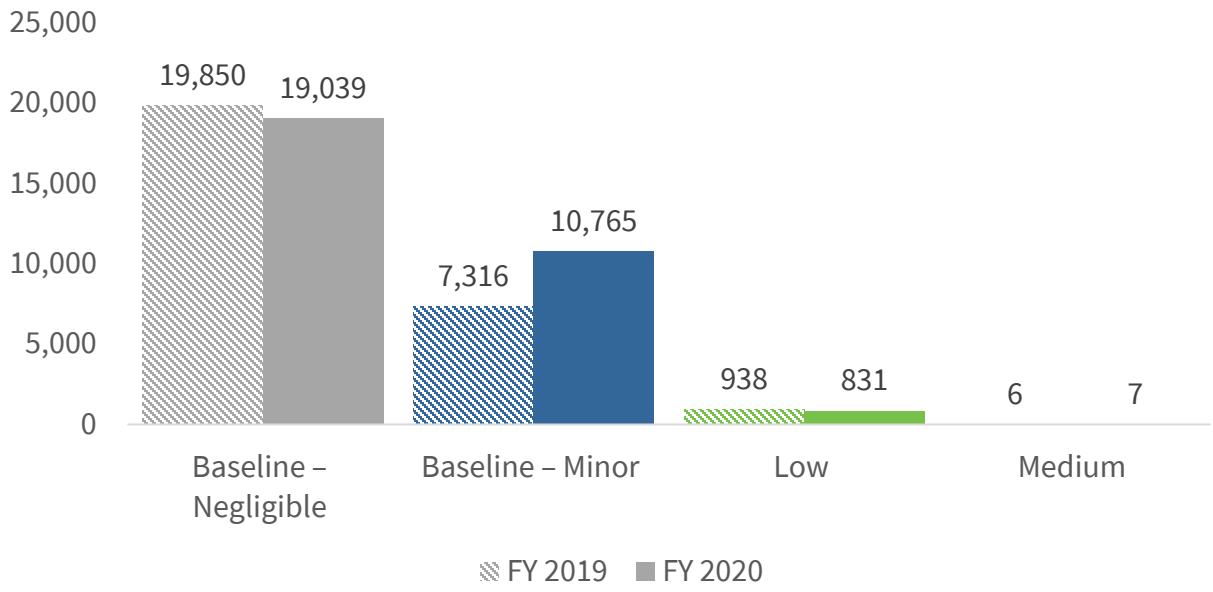
Source: Incidents reported to CISA in FY 2019 and FY 2020 under M-19-02 and M-20-04 respectively.

Incidents by NCISS Priority Level

When incidents are reported to CISA, the incidents are triaged and a priority level is calculated based on a variety of factors that include the level of impact.[11] The National Cyber Incident Scoring System (NCISS) is designed to provide 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 FY2020 and FY2019 for comparison, found in Table 7 and visualized in Figure 4.

The system is not intended to be an absolute scoring of the risk associated with an incident, but instead a relative mechanism for prioritization. It is not possible to conclude from this data whether there was a net increase or decrease in the risk level of reported incidents relative to the previous fiscal year. The vast majority of these incidents (accounting for approximately 97% in both fiscal years) were considered "Baseline", which per the Cybersecurity Incident Severity Schema are considered "unsubstantiated or inconsequential event[s]." OMB and CISA will continue to work with agencies to improve the quality of incident reporting data to ensure the risk of incidents is appropriately categorized, and with Congress to improve processes and definitions to provide the most pertinent information.

Figure 4 Agency-reported Incidents by NCISS Score



Source: Incidents reported to CISA in FY 2019 and FY 2020 under M-19-02 and M-20-04 respectively.

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

Table 7 Agency-reported Incidents by NCISS Priority Level

NCISS Priority Level	FY 2019	FY 2020
Uncategorized Incidents for which insufficient information was collected in order to provide an NCISS priority level.	471	177
Baseline – Negligible (White) Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. The potential for impact, however, exists and warrants additional scrutiny.	19,850	19,039
Baseline – Minor (Blue) Highly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	7,316	10,765
Low (Green) Unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	938	831
Medium (Yellow) May affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	6	7
High (Orange) Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	0	0
Severe (Red) Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	0	0
Emergency (Black) Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons.	0	0
Total	**28,581**	**30,819**

Source: Incidents reported to CISA in FY 2019 and FY 2020 under M-19-02 and M-20-04 respectively.

Major Incidents

Of the incidents reported by agencies in FY 2020, six incidents were determined by agencies to meet the threshold for major incidents in accordance with the definition in M-20-04. A summary of these major incidents is provided below:

Department of Defense

On September 4, 2020, Department of Defense reported a major incident at the Defense Manpower Data Center (DMDP) to Congress after a DMDC data analyst uploaded a dataset for secure internal delivery to a Navy civilian employee through the DMDC Request System

(DMDCRS), a secure file transfer application. Due to analyst error, the incorrect dataset was uploaded for delivery and a secondary review process failed to identify this mistake. The dataset included names, social security numbers, dates of birth, home addresses, personnel information, gender, and race. Upon receipt of the dataset in DMDCRS, the Navy employee promptly notified DMDC of the error and immediately deleted the information downloaded. Although the Navy civilian employee had approved access to DMDCRS and the dataset was transmitted securely within the DoD enclave, the Navy employee did not have a need-to-know for this particular dataset. The entire DMDC Data Delivery team received supplementary Privacy Act training, specifically highlighting proper procedural requirements and a reminder of the importance of appropriate handling of PII. In addition to this training, the DMDCRS team is developing additional safeguard proposals in an effort to prevent future occurrences. An estimated 300,000 individuals were potentially affected.

Department of Education

On July 9, 2020, Department of Education reported a major incident at Financial Student Aid (FSA) to Congress following the discovery that a shared drive which included files with borrower personally identifiable information (PII) was open and accessible to users within the Department. Within 24 hours of discovery, the Department restored proper file permissions to a more limited number of employees that required access. The Department found no evidence of improper use or external unauthorized disclosure of the PII. An estimated 304,668 individuals were potentially affected.

Department of Justice

On January 10, 2020, the Department of Justice (DOJ) reported a major incident at United States Marshals Service (USMS) to Congress after the Justice Security Operations Center (JSOC) detected an intrusion of the Detention Services Network (DSNet) system. Names, addresses, birth dates, social security numbers, FBI numbers, and alien numbers of current and former prisoners were successfully electronically exfiltrated through an SQL injection attack. Firewall rules were changed to block access outside of the Continental United States (CONUS), improvements were made to logging and detection systems used by USMS, the JSOC required all user accounts to be revalidated before users could access the DSNet system again, and the application itself has been corrected to properly validate user input. An estimated 387,000 individuals were potentially affected.

Department of Homeland Security

On October 25, 2019, DHS reported a major incident at the Federal Emergency Management Agency (FEMA) to Congress that involved possible overshare of PII data with a third-party vendor. PII data included full name, home address, phone number, e-mail address, and several non-PII elements related to disaster aid. The information was erroneously sent to a

vendor, which was in violation of the Information Sharing and Access Agreement (ISAA). The vendor has certified destruction of all email addresses. An estimated 307,000 individuals were potentially affected.

On February 2, 2020, DHS reported a major incident at FEMA to Congress involving improper storage, processing, and transfer of PII from the Housing Inspection Services Program by authorized vendors to an unaccredited server. PII data in the vendors' IT systems included names, addresses, telephone numbers, e-mail addresses, case numbers, professional license numbers, and fax numbers. The third-party assessor was unable to provide a breakdown of how many records within the respective vendor IT system contained PII, but it was able to determine that the unaccredited systems showed no indication of compromise. Remediation actions included: servers sanitization, data minimization, establishing external data transfer restrictions, and vendor contract modifications to address necessary compliance actions for applicable cybersecurity and data sharing policies. An estimated 6.8 million individuals were potentially affected.

On March 3, 2020, DHS reported a major incident at FEMA to Congress involving PII data stored within the Risk Analysis and Mapping System (RAMS) had improper access. Assessments revealed that access controls and the use of non-Government Furnished Equipment (GFE), when transmitting and storing data between 2007 and present, was substandard. Of the six vendors that have contractual agreements with FEMA to access RAMS, only one vendor contains applicable cyber security and privacy clauses for proper access. A third-party IT security vendor’s analysis of this vendor’s facility housing the affected system found no evidence of breach or compromise of vendor systems and that no PII was located on the vendor-owned systems. An estimated 2.5 million individuals were potentially affected.

D. Cybersecurity Risk Management

Risk Management Programs

An effective cybersecurity risk management program is integral to protecting information systems and data, as well as prioritizing technology investments. Federal agencies continue to struggle with establishing adequate information security risk management programs and aligning within the broader agency Enterprise Risk Management (ERM) programs.

Table 8 below, which includes the Government-wide average IG rating (out of 5, unless otherwise specified) for 8 metrics from FY 2017 to FY 2020, demonstrates limited improvement in the area of risk management. While some progress has been made since FY 2017, several of these metrics (12, 5, and 6 respectively) were the lowest scoring questions within the IG Metrics in FY 2020. There are many tools which can assist in the inventory and analysis of risks, however, few agencies have satisfactorily implemented them (as shown in 12).

In order to encourage the development of cybersecurity risk management programs, OMB and CISA must work together to update the FISMA process and integrate cybersecurity into the existing risk policy framework to focus on the measurement, reduction, and management of risk, rather than strictly compliance with relevant standards.

Table 8 IG Risk Management Ratings

IG Metric	FY2017	FY2018	FY2019	FY2020
5. To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk? (out of 3 in FY 2017, out of 5 in FY 2018-2020; added reference to SCRM in 2018)	2.3	2.5	2.4	2.6
6. To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain? (added reference to SCRM in 2019)	2.2	2.5	2.5	2.7
7. To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization?	2.8	2.9	2.9	3.1
9. To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks?	2.6	2.7	2.8	3.1
10. To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders?	2.7	2.8	2.9	3.1
12. To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards?	2.2	2.3	2.2	2.5

Source: Unweighted average rating (out of 5, unless otherwise noted) for independently assessed FY 2020 IG FISMA Metrics (or applicable year) representing 86 agencies in FY 2020

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 referred to as "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.

For FY 2020, 24 CFO Act agencies and 65 non-CFO Act agencies reported SAOP FISMA performance measures to OMB.

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

Executive Order 13800 recognizes that effective risk management requires agency heads 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 their respective agency, Executive Order 13719, *Establishment of the Federal Privacy Council* requires agency heads 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 implementing the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF).[12]

[12] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016) [hereinafter OMB Circular A-130].

Table 9 Senior Agency Officials for Privacy (SAOPs) and Privacy Programs

FY 2020 – SAOP FISMA Performance Measures[13]	CFO	Non-CFO
The head of the agency has designated an SAOP.[14]	100%	98%
Among the agencies that have designated an SAOP:		
The SAOP has the necessary role and responsibilities within the agency for compliance.[15]	100%	98%
The SAOP has the necessary role and responsibilities within the agency for policy making.[16]	100%	97%
The SAOP has the necessary role and responsibilities within the agency for risk management activities.[17]	100%	97%
The agency has developed and maintained a privacy program plan.[18]	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.[19]	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 ongoing awareness of their PII holdings and helps to ensure compliance with applicable privacy requirements and to manage privacy risks.

[13] Percentages are rounded to the nearest whole number throughout the SAOP performance measures.
[14] *See* OMB Memorandum M-16-24*, Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).
[15] *See id.*
[16] *See id.*
[17] *See id.*
[18] 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 structure of the privacy program, 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).
[19] *See id*. at Appendix I § 4(b)(1).

Table 10 Personally Identifiable Information Inventory

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains an inventory of the agency's information systems[20] that handle PII.[21]	100%	95%

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. However, SSNs are also key pieces of identifying information that potentially may 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 11 Collection, Maintenance, and Use of Social Security Numbers (SSNs)

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that collect, maintain, or use SSNs, the agency has an inventory of the agency's collection and use of SSNs.[22]	96%	88%
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.	91%	82%

[20] 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).

[21] *See* OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(a)(1)(a)(ii), 5(f)(1)(e) (July 28, 2016).

[22] 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.

The agency has developed and implemented a written policy to help ensure that any new collection or use of SSNs is necessary.	92%	71%
Among the agencies with such written policies:		
The agency's written policy provides specific criteria to use when determining whether the collection or use of SSNs is necessary.	100%	87%
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.	95%	89%
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.[23]	95%	88%

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 Risk Management Framework (RMF). The NIST RMF is a disciplined and structured process that Federal agencies use to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of information security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.

Table 12 Privacy and the NIST Risk Management Framework

FY 2020 – 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.[24]	100%	98%
Selection, implementation, and assessment of privacy controls.[25]	100%	89%

[23] *See* OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(f)(1)(f) (July 28, 2016).
[24] See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 3(a), 3(b)(5) (July 28, 2016).
[25] *See id.*

Authorization of information systems and common controls.[26]	100%	91%
Continuous monitoring of information systems that process PII.[27]	100%	85%
The agency has designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls.[28]	96%	68%
The agency has developed and maintained a written privacy continuous monitoring strategy.[29]	92%	71%
The agency has established and maintained an agency-wide privacy continuous monitoring program.[30]	79%	63%

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.

[26] *See id.*

[27] *See id.*

[28] *See id.* at Appendix I § 4(e)(5); *see also id.* at § 10(a)(14), (26), (66) and (86).

[29] 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).

[30] The SAOP is required to establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. *See* OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 4(d)(10)-(11), 4(e)(2) (July 28, 2016).

Table 13 Information Systems and Authorizations to Operate

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of information systems that handle PII that the agency authorized or reauthorized to operate during the reporting period.[31]	2,849	482
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.[32]	65%	87%
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.[33]	61%	81%
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.[34]	62%	82%
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.[35]	60%	84%

[31] 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).
[32] *See id*. at Appendix I § 4(a)(2), 4(e)(7).
[33] Federal agencies are required 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).
[34] *See id*. at Appendix I § 4(e)(3).
[35] *See id.* at Appendix I § 4(e)(9).

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 14 Information Technology Systems and Investments

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has a policy that includes explicit criteria for analyzing privacy risks when considering IT investments.[36]	79%	65%
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.[37]	67%	68%
The agency maintains an inventory of the agency's information technology systems that handle PII.	100%	95%

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.

[36] *See id.* at § 5(d)(3).
[37] *See id.* at § 5(a)(3)(e)(ii).

Table 15 Privacy Impact Assessments

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of IT systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) during the reporting period for which the agency is required to conduct a PIA under the E-Government Act of 2002.	5,101	748
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 under the E-Government Act of 2002 that are covered by an up-to-date PIA.[38]	3,601	580
Among the agencies that have a written policy for PIAs, the written policy for PIAs includes:[39]		
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%	94%
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%	92%
The agency has a process or procedure for:[40]		
Assessing the quality and thoroughness of each PIA.	100%	75%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	100%	77%
Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated.	96%	74%
Ensuring that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks.	96%	72%

[38] 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 altered 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).

[39] *See id.* at Appendix II § 5(e) (July 28, 2016).

[40] *See* OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix II § 5(e) (July 28, 2016).

F. Workforce Management

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

Table 16 Workforce Management

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency ensures that the agency's privacy workforce has the appropriate knowledge and skill.[41]	92%	92%
The agency has assessed its hiring, training, and professional development needs with respect to privacy during the reporting period.[42]	92%	88%
The agency has developed a workforce planning process to ensure that it accounts for privacy workforce needs.[43]	79%	72%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions.[44]	75%	72%

Table 17 Training and Accountability

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all Federal employees.[45]	100%	91%
The agency provides role-based privacy training to Federal employees with assigned privacy roles and responsibilities, including	75%	57%

[41] *See id.* at § 5(c)(2)
[42] *See id.* at § 5(c)(6).
[43] *See id.* at § 5(c)(1).
[44] *See id.*
[45] *See id.* at Appendix I § 4(h)(1).

managers, before authorizing their access to Federal information or information systems.[46]		
The agency has ensured measures are in place to test the knowledge level of information system users in conjunction with privacy training.[47]	96%	82%
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.[48]	96%	97%
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.[49]	100%	94%

Table 18 Contractors and Third Parties

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors.[50]	100%	86%
The agency has established rules of behavior, including consequences for violating rules of behavior, for contractors that have access to Federal information or information systems, including those that handle PII.[51]	100%	97%
Among the agencies that have established rules of behavior, the agency ensures that contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access.[52]	100%	95%
The extent to which the agency ensures that terms and conditions in contracts and other agreements involving the handling of Federal		

[46] *See id.* at Appendix I § 4(h)(5).
[47] *See id.* at Appendix I § 4(h)(1).
[48] *See id.* at Appendix I § 4(h)(6).
[49] *See id.* at Appendix I § 4(h)(7).
[50] *See id.* at Appendix I § 4(h)(1)-(2), (4)-(7).
[51] *See id.* at Appendix I § 4(h)(6).
[52] *See id.* at Appendix I § 4(h)(7).

information incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information:[53]		
Processes do not exist.	0%	5%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	13%	29%
Processes are fully documented and implemented and cover all relevant aspects.	25%	26%
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.	63%	40%
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:[54]		
Processes do not exist.	0%	2%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	0%	26%
Processes are fully documented and implemented and cover all relevant aspects.	21%	32%
Processes are fully documented and implemented and cover all relevant aspects, and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current.	79%	40%

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 includes, among other things, the composition of the agency's breach response team, the factors the agency shall consider when assessing the risk of harm to potentially affected individuals, and if, when, and

[53] *See id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).
[54] *See id.* at Appendix I § 4(j)(2)(a).

how to provide notification to potentially affected individuals and reporting to other relevant entities.[55]

Table 19 Breach Response

FY 2020 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that have a breach response plan, the breach response plan includes the agency's policies and procedures for:[56]		
Reporting a breach	100%	100%
Investigating a breach	100%	97%
Managing a breach	100%	97%
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.[57]	92%	89%
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.[58]	100%	91%
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.[59]	63%	55%
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that were reported within agencies during the reporting period.[60]	18,218	880
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.[61]	8,259	110

[55] *See* OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).
[56] *See id.* at § VII, XI.
[57] *See id.* at § X.B, XI.
[58] *See id.* at § VII.A, XI.
[59] *See id.* at § X.A, XI.
[60] *See id.* at § III.C, XI.
[61] *See id.* at § VII.D.1, XI.

The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that agencies reported to Congress during the reporting period.[62]	2,824	0
The total number of individuals potentially affected by the breaches reported to Congress during the reporting period.[63]	10,651,796	Not applicable

[62] *See id.* at § VII.D.3, XI.

[63] *See id.* at § XI.

Appendix I: Agency Cybersecurity Performance Summaries

This report promotes transparency and enhances accessibility to information on the unique missions, resources, and challenges of each agency by providing agency-specific narratives entitled "Cybersecurity Performance Summaries," which can be found here. Each summary contains four sections: CIO Rating, CIO Self-Assessment, Independent Assessment, and a count of incidents reported 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 2020 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**[64]**.**

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.

[64] 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 maturity model with five levels, as described in FY 2020 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
CAP Goals – Cross-Agency Priority Goals
CDM – Continuous Diagnostics and Mitigation Program
CEO – Chief Executive Officer
CFO – Chief Financial Officer
CIGIE – Council of the Inspectors General on Integrity and Efficiency
CIO – Chief Information Officer
CISO – Chief Information Security Officer
CSF – Cybersecurity Framework
CSP – Cloud Service Provider
DLP – Data Loss Prevention
DHS – Department of Homeland Security
ERM – Enterprise Risk Management
FedRAMP – Federal Risk and Authorization Management Program
FY – Fiscal Year
GFE – Government Furnished Equipment
GSA – General Services Administration
HVA – High Value Asset
HWAM – Hardware Assets Management
ICAM – Identity, Credential, and Access Management
ISCM – Information Security Continuous Monitoring
IG – Inspector General
NCPS – National Cybersecurity Protection System
NIST – National Institute of Science and Technology
OFCIO – Office of the Chief Information Officer
OIG – Office of the Inspector General
OMB – Office of Management and Budget
PII – Personally Identifiable Information
PIV – Personal Identity Verification
POA&M – Plan of Actions and Milestones
RMF – Risk Management Framework
RVA – Risk and Vulnerability Assessment
SAOP – Senior Agency Official for Privacy
SAR – System Architecture Review
SCAP – Security Content Automation Protocol
SMTP – Simple Mail Transfer Protocol
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