Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2018

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 (Dec. 18, 2014) (codified at 44 U.S.C. § 3553). This report also incorporates the OMB's analysis of agency application of the intrusion detection and prevention capabilities, as required by Section 226 of the Cybersecurity Act of 2015 (Pub. L. No. 114-113). OMB obtained information from the Department of Homeland Security (DHS), and Chief Information Officers and Inspectors General from across the Executive Branch to compile this report. This report primarily includes Fiscal Year 2018 data reported by agencies to OMB and DHS on or before October 31, 2018.

Table of Contents

Executive Summary:
The State of Federal Cybersecurity

The cybersecurity threats facing the Federal Government, and our Nation as a whole, clearly demonstrate the need for vigilance to protect the country's data and digital infrastructure. America's networks, both public and private, remain top targets of malicious actors the world over. This environment demonstrates that effective cybersecurity requires any organization — whether a Federal agency or a public or private company — to identify, prioritize, and manage cyber risks across its enterprise.

This Administration has placed a clear priority on cybersecurity. In September 2018, the President released the National Cyber Strategy to defend the homeland and promote American prosperity by not only protecting public and private systems and information, but promoting a secure digital economy. The first fully articulated cybersecurity strategy in 15 years, the National Cyber Strategy builds and expands upon the work begun under Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (Executive Order 13800) released in May 2017, which enhanced cybersecurity risk management across the Federal Government. Executive Order 13800 recognizes that the Government must ensure that it can secure citizens' information and that agencies can deliver on their core missions and services even as malicious cyber actors seek to disrupt those services. Cybersecurity is also a critical component of the President's Management Agenda, with the Cross-Agency Priority Goal on Modernizing IT to Increase Productivity and Security not only tracking agency progress implementing key security capabilities, but also helping to revolutionize the way the Federal Government approaches cybersecurity.

Although this progress is encouraging, agencies still endured 31,107 cybersecurity incidents in Fiscal Year (FY) 2018. This is a 12% decrease over the 35,277 incidents that agencies reported in FY 2017. However, FY 2018 marked the first year since the creation of the major incident[1] designation that no incidents met the threshold. The Federal Government must continue to act to reduce the impact that cybersecurity incidents have on the Federal enterprise. Accordingly, this annual report to Congress on the implementation of the Federal Information Security Modernization Act of 2014 highlights government-wide programs and initiatives as well as agencies' progress to enhance Federal cybersecurity over the past year and into the future.

[1] As defined in OMB Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*

A. Federal Cybersecurity Roles and Responsibilities

The Federal Information Security Modernization Act of 2014 (FISMA) identifies the agency head as the responsible official for her or his respective organization's cybersecurity posture, and Executive Order 13800 reinforces this responsibility. Enhancing Federal cybersecurity is a collective effort that requires participation from personnel across the Federal enterprise. The following section provides a brief overview of key agencies' roles and responsibilities in strengthening Federal cybersecurity in accordance with statute, policy, or the agency's mission:

Office of Management and Budget (OMB): OMB is responsible for overseeing Federal agencies' information security and privacy practices and for developing and directing implementation of policies and guidelines which support and sustain those practices. Within OMB, these responsibilities are delegated to the Office of the Federal Chief Information Officer (OFCIO), with the Federal Chief Information Security Officer leading the Cybersecurity team that works with Federal agency leadership to address information security priorities. OFCIO 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. The Office of Information and Regulatory Affairs is responsible for providing assistance to Federal agencies on privacy matters, developing Federal privacy policy, and overseeing implementation of privacy policy by Federal agencies.

National Security Council (NSC): NSC is the Executive Office of the President component responsible for coordinating policy initiatives with the President's senior advisors, cabinet officials, and military and intelligence community advisors. The NSC Cybersecurity Directorate fulfills this role for cybersecurity issues, advising the President from a national security and foreign policy perspective. NSC and OMB coordinate and collaborate with Federal agencies to implement the Administration's cybersecurity priorities.

Department of Homeland Security (DHS): DHS is the operational lead for Federal cybersecurity and has the authority to coordinate government-wide cybersecurity efforts, issue binding operational directives (BODs) detailing actions that agencies should take to improve their cybersecurity, and provide operational and technical assistance to agencies, including through the operation of the Federal information security incident center. Under FISMA and other authorities, DHS provides common security capabilities for agencies through the National Cybersecurity Protection System (which includes the EINSTEIN program) and Continuous Diagnostics and Mitigation (CDM) program and provides incident response assistance through the National Cybersecurity and Communications Integration Center (NCCIC) in accordance with Presidential Policy Directive-41, United States Cyber Incident Coordination. DHS also facilitates information sharing across the Federal Government 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' use. GSA also operates the Centers of Excellence, which provide expert advice, consulting, development and support solution implementation in the areas of: Cloud Adoption; IT Infrastructure Optimization; Customer Experience; Service Delivery Analytics; and Contact Centers. GSA also hosts 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 bureau of the Department of Commerce, is charged with developing 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 provides management, operational, and technical security guidelines on a broad range of topics, including incident handling and intrusion detection, supply chain risk management, and strong authentication. Additionally, NIST develops and updates the Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

Federal Bureau of Investigations (FBI): The FBI is the component of the Department of Justice responsible for leading 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, and partnerships with Federal, state, and local law enforcement, and cybersecurity organizations.

Federal Agencies: FISMA requires that Federal agency heads be responsible for the security of Federal information and information systems at their respective agencies. Each agency head may delegate this authority to his or her respective Chief Information Officer (CIO) and/or Senior Agency Information Security Official, a role commonly filled by the Chief Information Security Officer (CISO). Agencies are ultimately responsible for allocating the necessary people, processes, and technology to protect Federal data.

The Intelligence Community: An essential component of cybersecurity is obtaining and analyzing information on the threats and malicious actors targeting both public and private infrastructure. Led by the Office of the Director of National Intelligence, the Intelligence Community provides indispensable information to the Federal Government and encompasses the work of 17 agencies, including the National Security Agency and Central Intelligence Agency.

Section I: Federal Cybersecurity Activities

A. Executive Priorities

The President has made strengthening the Nation's cybersecurity a priority from the outset of this Administration. In May 2017, the President signed Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which concentrates on IT modernization and cybersecurity risk management. Executive Order 13800 reinforces FISMA by holding agency heads accountable for managing cybersecurity risks to their enterprises[2] and requiring each agency to assess its cybersecurity risks and submit a plan to OMB detailing actions to implement the NIST Cybersecurity Framework.[3]

As part of the Executive Order 13800 implementation effort, the White House issued two strategic deliverables. The *Report to the President on Federal IT Modernization*, details activities to modernize and safeguard high-risk High Value Assets (HVAs), promotes the consolidation of network acquisitions and management, and prompts agencies to leverage commercial cloud solutions and cybersecurity shared services where available.

The second deliverable, the *Federal Cybersecurity Risk Determination Report and Action Plan*, assesses the state of agencies' cybersecurity risk management efforts and includes a plan for addressing these areas of risks. The four core actions identified for reducing cybersecurity risk were: (1) Increasing cybersecurity threat awareness; (2) Standardizing cybersecurity and IT capabilities; (3) Maturing Security Operations Centers (SOCs); and (4) Driving agency accountability. Throughout 2018, OMB, DHS, and the broader Federal IT and cybersecurity community have taken concrete steps toward achieving these actions. The following overview of the Federal Government's cybersecurity activities in FY 2018 is organized in alignment with the actions from this report.

B. Increasing Cybersecurity Threat Awareness

Numerous government and industry cybersecurity reports highlighted how threat actors employ persistent and increasingly sophisticated techniques to attack and compromise information systems. Gathering, analyzing, and disseminating this information is vital to

[2] FISMA requires agencies to implement information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of "information collected or maintained by or on behalf of [an] agency" and "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency". 44 U.S.C. § 3554.

[3] NIST published Draft NIST Interagency Report 8170 in support of Executive Order 13800 in May 2017, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*. Available at: https://csrc.nist.gov/CSRC/media/Publications/nistir/8170/draft/documents/nistir8170-draft.pdf

effectively managing government cybersecurity risk, however operationalizing the information has proven to be challenging for the Federal enterprise. In working to address this challenge, OMB and DHS continue to work together to improve the quality, effectiveness, and scale of the government's threat-related programs.

Cyber Threat Framework

To enable agencies to better understand the ways threat actors seek to gain access to Federal networks, systems, and data, OMB Memorandum M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements, directed DHS, in coordination with OMB and the Department of Defense, to help agencies implement the Director of National Intelligence's (ODNI) Cyber Threat Framework. Specific actions identified in the memo include:

1. Develop and implement a solution that leverages threat intelligence to identify deficiencies in agency security capability coverage against adversarial activity (e.g. heat mapping).
2. Support agencies in identifying and assessing their security capability coverage on High Value Assets (HVAs)
3. Enable agencies to use the solution to prioritize cybersecurity investments based on threat-informed risk management, with specific focus on HVAs

The adoption of this framework is intended to enable the implementation of the proceeding capabilities so that agency cybersecurity risk decisions better informed by threat intelligence.

National Cybersecurity Protection System (including EINSTEIN)

The National Cybersecurity Protection System, of which the EINSTEIN system is a key 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 (E^3A), an integrated intrusion prevention, detection, analysis, and information sharing system that builds on the passive detection capabilities of EINSTEIN 1 and EINSTEIN 2. The E^3A program also serves as a platform to aggregate Federal civilian executive branch traffic so that DHS can implement new and advanced protections. As of September 26, 2018, DHS reports that, of 102 Federal civilian agencies, 70 report implementing all three NCPS capabilities, including all 23 CFO Act agencies.

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

EINSTEIN Capability	● Complete	◑ In Progress	◌ Deferred[4]	○ Not Implemented
E1/E2	74	0	0	28
CFO	23	0	0	0
Non-CFO	51	0	0	28
E3A Email	70	6	8	18
CFO	23	0	0	0
Non-CFO	47	6	8	18
E3A DNS	81	4	1	16
CFO	23	0	0	0
Non-CFO	58	4	1	16

C. Standardizing Cybersecurity and IT Capabilities

Agency risk assessments have shown that insufficient standardization and insufficient access to common capabilities have hindered agencies' ability to mitigate vulnerabilities and other cybersecurity challenges. The High Value Asset (HVA) program, Identity, Credential, and Access Management (ICAM) program, Trusted Internet Connection (TIC) program, and Continuing Diagnostics and Mitigation (CDM) program have all undergone review over the last year in order to incorporate new technologies and processes while driving toward more standardized and effective cybersecurity capabilities.

Continuous Diagnostics and Mitigation (CDM)

The CDM program provides tools and capabilities to agencies that allow them to gain visibility into their IT environments and better manage cybersecurity risk through increased awareness. It is essential that agencies maintain visibility into their IT environments to identify and mitigate vulnerabilities, detect suspicious behavior, and respond to threats in a manner that is rapid and efficient. All 23 civilian CFO Act agencies currently report data, in

[4] The agency faces a technical challenge to implement email filtering for its third party, cloud-based email service. DHS continues to work with the affected agencies and their E3A service provider to engineer solutions.

near-real time, to their respective agency dashboards using data generated from CDM Phase 1 asset management tools.

During FY 2018, the CDM program office also successfully established data exchanges between all 23 civilian CFO Act agency dashboards and the Federal dashboard, which is hosted at the DHS National Cybersecurity and Communications Integration Center (NCCIC). Additionally, the CDM program office connected almost a dozen non-CFO Act agencies to the CDM Shared Services Platform and worked to onboard more than 40 additional non-CFO Act agencies. Furthermore, the CDM program office has made Phase 3 boundary protection, event management, and security lifecycle tools available to 96% of participating agencies through the CDM DEFEND contract.

OMB M-19-02[5] addresses gaps in tool deployment and enterprise visibility by including several actions for the CDM program office, and the memo allows agencies to acquire continuous monitoring tools outside of the CDM program if they can provide OMB and DHS with sufficient justification. However, even if agencies acquire tools from outside of the CDM contract vehicle, they must provide certain defined information to the Federal Dashboard.

High Value Assets (HVAs)

An essential element of a risk-based approach to cybersecurity is the understanding that not all IT and information assets possess the same value to an organization or the actors seeking to compromise them. Among the recommendations set forth in previous OMB and DHS guidance and policies were revising NIST's Federal Information Processing Standard (FIPS) Publications 140-2, 199, and 200, updating the annual FISMA CIO metrics to track controls for HVAs, and developing a playbook for agencies as they manage their systems in a prioritized, risk-based approach. In November 2018 OMB released *OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*. The guidance provides direction for:

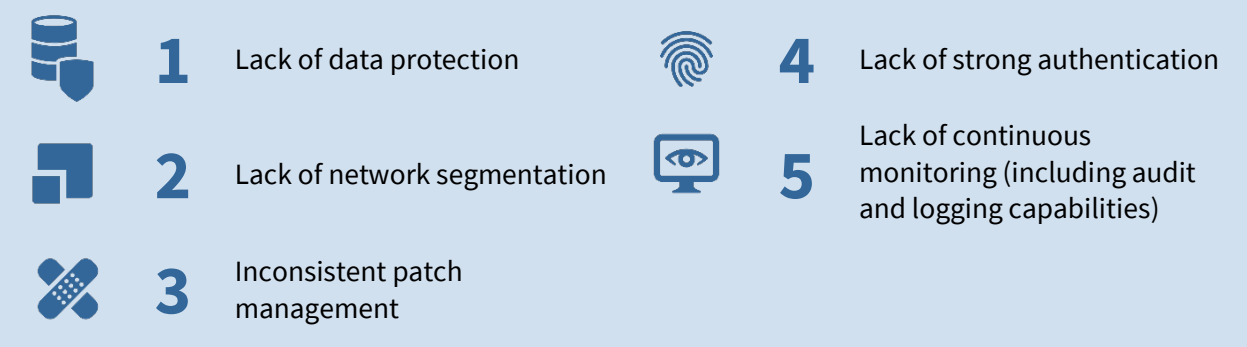
- Enhancing the HVA initiative, creating a formal program that supports all agencies, including both CFO Act and non-CFO Act agencies, in HVA identification, assessment, remediation, and response to incidents.
- Instituting a simplified definition and data-driven methodology for identifying and prioritizing HVAs across the Federal Government.

[5] OMB Memorandum M-19-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements

- Implementing NIST SP 800-160 security engineering principles to ensure that HVAs are developed with cybersecurity resiliency in mind.
- Establishing a regular process to develop and disseminate contract clauses that agencies can leverage to incorporate security requirements for HVAs as part of the procurement process.
- Consolidating and updating previous requirements from OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, and OMB memorandum M-17-09, *Management of Federal High Value Assets*, and rescinding those memoranda.

In FY 2018, DHS conducted 61 HVA assessments, resulting in 356 findings (221 System Architecture Review findings and 135 Risk and Vulnerability Assessment findings). These assessments revealed that the Federal Government's continues to face challenges mitigating basic security vulnerabilities. The most common security deficiencies identified across the HVA landscape are identified in Figure 1.

Figure 1 Top 5 HVA findings in FY 2018



Trusted Internet Connections

Another priority raised specifically in the Report to the President on the Modernization of Federal IT was to update the Trusted Internet Connections (TIC) program. The purpose of the TIC initiative is to enhance network security across the Federal Government. Historically, this has been accomplished by routing Federal internet traffic through a limited number of access points at which security measures were deployed. While the initiative has accomplished some of its security goals, changes to the way the Federal Government utilizes technology, particularly its increased use of cloud-based infrastructure, necessitated an update to the program. To accomplish this, OMB worked in close collaboration with DHS, GSA, and a select set of agencies to initiate and oversee TIC modernization pilots. These pilots seek to deliver similar security benefits as the TIC program while allowing greater flexibility in delivering IT

services. The results of these pilots have been used to inform the future direction of the TIC initiative. Three primary goals of the updated TIC initiative are to:

- Remove Barriers to Cloud and Modern Technology Adoption – Agencies will have increased flexibility in how they meet TIC initiative security objectives. In some cases, the TIC initiative may entail implementing alternative security controls rather than routing traffic through a physical TIC access point.
- Ensure the TIC Initiative Remains Agile – Due to the rapid pace that technology and cyber threats evolve, the TIC initiative includes a collaborative and iterative process, which includes input from both industry and Federal agencies, for continuously updating the TIC initiative's implementation guidance. This process includes ongoing piloting and approval of new and innovative methods to achieve TIC Initiative security objectives in the most effective and efficient manner.
- Streamline and Automate Verification Processes – The goal is to shift from burdensome, point-in-time, manual spot checks to a scalable, comprehensive, and continuous validation process.

As part of the updated TIC initiative, expected to be released in FY 2019, DHS will define TIC initiative requirements in documentation called TIC Use Cases. The TIC Use Case documentation will outline which alternative security controls, such as endpoint and user-based protections, must be in place for specific use cases where traffic is not required to flow through a physical TIC access point. Agencies are required to meet the requirements detailed in the TIC Use Cases guidance.

Identity, Credential, and Access Management

Digital identity is foundational to the delivery of services in support of agency missions. Pursuant to recommendations outlined in the Report to the President on Federal IT Modernization, OMB released a draft identity policy for public comment, with the final version of the guidance issued on May 24, 2019. Among the guidance's goals were to reduce agency burden and identify service areas suitable for shared services. Following the conclusion of the public comment period, OMB worked across the interagency and private industry to refine the guidance, resulting in a comprehensive update to ICAM. The updated guidance enabled the following:

- Empowers the Federal Government to achieve a strong foundation for identity management by directing actions to remove blockers that inhibit innovation.
- Aligns with the National Cyber Strategy and forthcoming Cloud Smart policy, providing guidance to strengthen the approach for end-to-end identity lifecycle

management and the approach to identity management across Federal cloud services.

- Promotes an Identity-centric perspective for managing devices, Non-Person Entities (NPE), Robotics Process Automation (RPA) and broader use of Artificial Intelligence and Deep Learning.
- Adapts the approach for achieving the goals of Homeland Security Presidential Directive-12 that may extend beyond the current implementation of Personal Identity Verification (PIV) credentials
    - NIST, OMB and the interagency are currently in the process of refining Federal Information Processing Standard (FIPS) 201 which provides the standard for PIV.
    - Additional updates to NIST Special Publications (SPs) and references documents such as the Federal ICAM (FICAM) playbooks are in process.
- Strengthens identity proofing by directing the establishment of privacy-enhanced APIs to improve verification. This includes working with agencies to reduce the over-reliance on SSN, and improving the security and privacy of data provided by the public.

Through the Federal CIO community, OMB and the interagency are supporting a set of pilot activities to inform development and to drive federated architectures centered on strong identity management (e.g., Zero Trust). These efforts are driven by a resurgence in public-private partnership in tackling key issues for agencies as they drive to more modern architectures.

D. Maturing Security Operations Centers (SOCs)

As noted in the Risk Determination Report and Action Plan, Federal agencies often lack the full visibility into their networks necessary to effectively detect data exfiltration attempts and respond to cybersecurity incidents. This in part stems from an insufficient number of fulltime employees with the requisite skills to operate a SOC effectively, however, at larger agencies, it is often also a result of numerous SOCs that do not effectively communicate with each other. This fractured security landscape can be a significant impediment and contribute to diminished network visibility and inefficient and ineffective operations.

In order to combat this challenge, OMB M-19-02 commits OMB and DHS to working with agencies to assess and enhance the maturity of their SOCs and streamline security operations across their enterprise. The memo requires agencies to provide to OMB and DHS a Cybersecurity Operations Maturation Plan in which they either consolidate their SOCs, enhance their SOC(s) to a certain level of maturity, or migrate to a managed service by the

end of FY 2020. The memo includes several criteria for inclusion in the Maturation Plan in order to continue to standardize, centralize, and provide visibility of agency cybersecurity capabilities across the enterprise.

E. Driving Agency Accountability

While the priority placed on Federal cybersecurity has been clear, metric-based, proactive oversight is necessary to both measure the progress agencies make over time as well as hold agency leaders accountable when they fail to meet established targets. Pursuant to EO 13800, OMB developed a Risk Management Assessment process to help agencies understand and decrease their cybersecurity risk. OMB has also aligned its various oversight processes to the NIST Cybersecurity Framework to facilitate important conversation across and between organizations.

Cybersecurity Budgeting

The Federal Government continues to improve its overall cybersecurity posture. However, in order for agencies to make risk-informed budget decisions, they must have a better understanding of how each incremental dollar reduces risk to their agency. Accordingly, OMB is working to develop reporting structures to capture agency spending and budget information at the cybersecurity capability level. The reporting structure is aligned against the NIST Cybersecurity Framework as well as the FISMA CIO metrics used to evaluate the degree to which agencies are managing their cybersecurity risk. This allows a common vocabulary and taxonomy as agencies make difficult resourcing decisions. OMB has worked with agencies to integrate these structures into strategic planning and risk management discussions with agency CIOs, CISOs, and CFOs.

A summary of unclassified cybersecurity spending for FY 2018 can be found in Table 2 below. These figures include spending related to protecting information and information systems. However, a number of agencies also have cybersecurity-related spending that is not dedicated to the protection of their own networks, serving instead a broader cybersecurity mission. For instance, to ensure a consistent baseline level of information security, there are a number of programs that provide tools and capabilities government-wide, such as DHS' CDM program. Additionally, numerous programs exist that further enhance national and Federal cybersecurity focused on areas such as standards, research, and the investigation of cyber-crimes rather than specific technical capabilities. There are also types of cybersecurity that are not covered in the table, including classified spending.

Table 2 FY 2018 Cybersecurity Spending

Agency	FY 2018 Spend ($ Millions)	Agency	FY 2018 Spend ($ Millions)
Commerce	$349.7	NASA	$170.7
DHS	$1,858.9	NRC	$24.6
DOD	$8,048.0	NSF	$246.7
DOT	$184.8	OPM	$38.5
ED	$103.8	SBA	$9.1
Energy	$447.9	SSA	$167.1
EPA	$21.1	State	$361.5
GSA	$71.6	Treasury	$445.3
HHS	$359.0	USAID	$43.8
HUD	$14.9	USDA	$261.7
Interior	$87.9	VA	$385.9
Justice	$820.8	Non-CFO Act	$361.8
Labor	$92.9		
		Total	**$14,978**

Binding Operational Directives (BODs)

Per FISMA, DHS has the authority to issue compulsory directives to Federal agencies known as Binding Operational Directives (BODs). In line with OMB's policies, principles, standards, and guidelines, BODs seek to safeguard Federal information and information systems from known or reasonably suspected information security threats, vulnerabilities, or risks. The Cybersecurity and Infrastructure Security Agency's Federal Network Resilience Division leads DHS efforts to develop, communicate, and manage actions and critical activities related to all BODs. Since acquiring this authority, DHS has issued seven BODs to address vulnerabilities impacting Federal agencies, including two in FY 2018:

- BOD 18-01: Enhance Email and Web Security: Email-based threats remain one of the most prominent attack vectors for Federal agencies. By implementing specific security standards that have been widely adopted in industry, DHS determined that the Federal enterprise as a whole could enhance the integrity and confidentiality of internet-delivered data, minimize spam, and better protect users who might

otherwise fall victim to phishing emails seemingly from government-owned system. BOD 18-01 requires agencies to take several actions related to email and web security, including implementing best practices related to STARTTLS, DMARC and HSTS. It included staggered deadlines for implementing a variety of actions, all ranging from 30 days to 1 year of BOD issuance on October 16, 2017.

- BOD 18-02: Securing High Value Assets: To ensure effective identification and timely identification of risks and remediation of major and critical security weaknesses to HVA systems, BOD 18-02 requires all agencies to identify and submit prioritized lists of their HVAs to DHS. Once DHS received these lists, DHS and OMB created a prioritized government-wide list based on various factors. Once the list was established, agencies selected by OMB and DHS would undergo one or more assessments to identify security weaknesses. BOD 18-02 also requires agencies to remediate identified security weaknesses and provide a plan of action and milestones as well as mitigation progress within 30 days of issuance of an HVA assessment report.

Enhancing Cybersecurity Oversight

Consistent with their other efforts to help agencies understand their cybersecurity risk profiles, OMB and DHS have continued to work with the CIO and Inspectors General (IG) communities to align program oversight practices and FISMA metrics with the NIST Cybersecurity Framework's five function areas of Identify, Protect, Detect, Respond, and Recover. This has included the development of the IG Cybersecurity Capability Maturity Model (CMM) and corresponding Evaluation Guide, which provides agencies with an evolving list of evidence that IGs can use to evaluate each stage of maturity within their CMM. The Evaluation Guide directly addresses the recommendation provided in the Government Accountability Office report Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (GAO-17-549), in which OMB, in cooperation with DHS, the CIO Council, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) was directed to work toward ensuring consistent and comparable CMM results across all Federal agencies.

Section II: 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 "processes") personally identifiable (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 2018, all 24 CFO Act agencies and 61 non-CFO Act agencies reported SAOP FISMA performance measures to OMB.

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

Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 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 No. 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, contractor and third parties, workforce, training, incident response, and implementing the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF).[6]

[6] 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 3 Senior Agency Officials for Privacy (SAOPs) and Privacy Programs

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The head of the agency has designated an SAOP.[7]	100%	100%
The SAOP has the necessary role and responsibilities to ensure compliance with applicable privacy requirements.[8]	100%	97%
The SAOP has the necessary role and responsibilities to develop and evaluate privacy policy.[9]	100%	97%
The SAOP has the necessary role and responsibilities to manage privacy risks consistent with the agency's mission.[10]	100%	98%
The agency has a privacy program plan.[11]	100%	87%
The agency identifies and plans for the resources needed to implement the agency's privacy program.[12]	96%	82%

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.

[7] *See* OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).
[8] *See id.*
[9] *See id.*
[10] *See id.*
[11] 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).
[12] *See id*. at Appendix I § 4(b)(1).

Table 4 Personally Identifiable Information Inventory

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains an inventory of the agency's information systems[13] that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[14]	100%	97%

In addition to ensuring compliance and managing the privacy risks associated with PII generally, Federal agencies are required to take additional steps to manage the risk associated with the collection, maintenance, and use of Social Security numbers (SSNs). The Federal Government uses SSNs as unique identifiers for many purposes, 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. As such, Federal agencies are required to eliminate the unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as a personal identifier.

Table 5 Collection, Maintenance, and Use of Social Security numbers (SSNs)

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has an inventory of the agency's collection and use of SSNs.[15]	100%	94%
The agency maintains its inventory of SSNs as part of the agency's inventory of information systems.	96%	88%
The agency has developed and implemented a written policy to ensure that any new collection or use of SSNs is necessary.	88%	69%
The agency's written policy provides specific criteria to use when determining whether the collection or use of SSNs is necessary.	90%	88%

[13] 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).

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

[15] 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's written policy establishes a process to ensure that any collection or use of SNNs remain necessary over time.	90%	83%
If the agency has not successfully eliminated all unnecessary collections and uses of SSNs at the agency, the agency took steps during the reporting period to eliminate the unnecessary collection and use of SSNs.[16]	100%	95%

C. Privacy and the Risk Management Framework

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

Table 6 Privacy and the NIST Risk Management Framework

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency implemented a risk management framework to guide and inform the following: Categorization of Federal information and information systems that process PII.[17]	96%	98%
Selection, implementation, and assessment of privacy controls.[18]	96%	92%
Authorization of information systems and common controls.[19]	96%	90%
Continuous monitoring of information systems that process PII.[20]	96%	73%
The SAOP designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency.[21]	96%	59%

[16] *See* OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(f)(1)(f) (July 28, 2016).
[17] See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 3(a), 3(b)(5) (July 28, 2016).
[18] *See id.*
[19] *See id.*
[20] *See id.*
[21] *See id.* at Appendix I § 4(e)(5); *see also id.* at § 10(a)(14), (26), (66) and (86).

The agency has developed and maintains a written privacy continuous monitoring strategy.[22]	79%	69%
The agency has established and maintains an agency-wide privacy continuous monitoring program.[23]	67%	54%

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.

[22] 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).

[23] 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 7 Information Systems and Authorizations to Operate

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of information systems that process PII that were authorized or reauthorized to operate during the reporting period.[24]	2,234	276
Information systems that process PII that were authorized or reauthorized during the reporting period where an SAOP reviewed and approved the information system's categorization.[25]	71%	89%
Information systems that process PII that were authorized or reauthorized during the reporting period where an SAOP reviewed and approved a system privacy plan prior to authorization or reauthorization.[26]	71%	81%
Information systems that process PII that were authorized or reauthorized during the reporting period where an 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.[27]	72%	82%
Information systems that process PII that were authorized or reauthorized during the reporting period where an 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.[28]	75%	88%

[24] 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 II § 4(j)(2)(c) (July 28, 2016).

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

[26] 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).

[27] *See id*. at Appendix I § 4(3).

[28] *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 8 Information Technology Systems and Investments

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has a policy that includes explicit criteria for analyzing the privacy risks when considering IT investments.[29]	67%	56%
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 for IT resources that will be used to process PII.[30]	71%	64%
The agency maintains an inventory of information technology systems that process PII.	100%	95%

E. 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 privacy impact assessments (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.

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

Table 9 Privacy Impact Assessments

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The number of IT systems maintained, operated, or used by an agency (or by an entity on behalf of the agency) during the reporting period for which a PIA is required.	3,575	762
IT systems maintained, operated, or used by an agency (or by an entity on behalf of the agency) that are covered by an up-to-date PIA.[31]	3,057	665
The agency has a written policy for privacy impact assessments that includes:[32] A requirement that a PIA be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA.	96%	100%
A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs.	96%	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.	96%	94%
The agency has a process or procedure for each of the following:[33] Assessing the quality and thoroughness of each PIA.	96%	81%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	96%	73%
Monitoring the agency's IT systems and practices to determine when and how PIAs should be updated.	96%	73%
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%	77%

F. Workforce Management

Federal agencies' privacy programs are required to play a key role in workforce management activities and holding agency personnel accountable for complying with applicable privacy

[31] 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).

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

[33] *See id.*

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 10 Workforce Management

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency ensures that its privacy workforce has the appropriate knowledge and skill.[34]	96%	93%
The agency assessed its hiring, training, and professional development needs with respect to privacy during the reporting period.[35]	83%	87%
The agency has developed a workforce planning process to ensure that it accounts for its privacy workforce needs.[36]	67%	66%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions.[37]	67%	57%

Table 11 Training and Accountability

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all Federal employees.[38]	100%	93%
The agency provides role-based privacy training to Federal employees employed by the agency with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties.[39]	71%	51%
The agency has measures in place to test the knowledge level of information system users in conjunction with privacy training.[40]	92%	66%

[34] *See id.* at § 5(c)(2)
[35] *See id.* at § 5(c)(6).
[36] *See id.* at § 5(c)(1).
[37] *See id.*
[38] *See id.* at Appendix I § 4(h)(1).
[39] *See id.* at Appendix I § 4(h)(5).
[40] *See id.* at Appendix I § 4(h)(1).

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 process PII.[41]	100%	95%
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 access being granted.[42]	96%	91%

Table 12 Contractors and Third Parties

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors.[43]	100%	85%
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 process PII.[44]	100%	92%
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.[45]	100%	95%
The extent to which the agency ensures that terms and conditions in contracts and other agreements involving the processing 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.[46] Procedures or processes are generally informal, incomplete, and inconsistently applied.	0%	8%
Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.	8%	21%
Procedures and processes are fully documented and implemented and cover all relevant aspects.	46%	44%

[41] *See id.* at Appendix I § 4(h)(6).
[42] *See id.* at Appendix I § 4(h)(7).
[43] *See id.* at Appendix I § 4(h)(1)-(2), (4)-(7).
[44] *See id.* at Appendix I § 4(h)(6).
[45] *See id.* at Appendix I § 4(h)(7).
[46] *See id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).

Procedures and processes are fully documented and implemented and cover all relevant aspects and reviews are regularly conducted to assess the effectiveness of the procedures and processes and to ensure that documented policies remain current.	46%	26%
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.[47] Procedures or processes are generally informal, incomplete, and inconsistently applied.	8%	7%
Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.	20%	5%
Procedures and processes are fully documented and implemented and cover all relevant aspects.	45%	54%
Procedures and processes are fully documented and implemented and cover all relevant aspects and reviews are regularly conducted to assess the effectiveness of the procedures and processes and to ensure that documented policies remain current.	27%	34%

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 of 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 how to provide notification to potentially affected individuals and other relevant entities.[48]

Table 13 Incident Response

FY 2018 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency has a breach response plan that includes the agency's policies and procedures for each of the following:[49]	100%	100%
Reporting a breach		
Investigating a breach	96%	98%
Managing a breach	100%	98%

[47] *See id.* at Appendix I § 4(j)(2)(a).
[48] *See* OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).
[49] *See id.* at § VII, XI.

The SAOP reviewed the agency's breach response plan during the reporting period to ensure that the plan was current, accurate, and reflected any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology.[50]	100%	95%
The agency has a breach response team composed of agency officials designated by the head of the agency that may be convened to lead the agency's response to a breach.[51]	100%	87%
The members of the agency's breach response team participated in at least one tabletop exercise during the reporting period.[52]	67%	55%
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that were reported within agencies during the reporting period.[53]	20,887	722
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that agencies principal security operations centers reported to US-CERT during the reporting period.[54]	9,838	131
The number of breaches, as OMB Memorandum M-17-12 defines the term "breach," that agencies reported to Congress during the reporting period.[55]	2,128	1
The total number of individuals potentially affected by the breaches reported to Congress during the reporting period.[56]	117,572	2

[50] *See id.* at § X.B, XI.
[51] *See id.* at § VII.A, XI.
[52] *See id.* at § X.A, XI.
[53] *See id.* at § III.C, XI.
[54] *See id.* at § VII.D.1, XI.
[55] *See id.* at § VII.D.3, XI.
[56] *See id.* at § XI.

Section III: FY 2018 Agency Performance

A. Introduction to 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 are found in subsection C below. Each summary contains four sections: CIO Rating, CIO Self-Assessment, Independent Assessment, and a count of US-CERT incidents by attack vector. The descriptions below provide an overview of the sections included in each agency performance summary.

CIO Self-Assessments

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.

Independent Assessments[57]

This independent narrative section allows IGs (or independent assessors)[58] to frame the scope of their analysis, identify key findings, and provide high level recommendations to address those findings.

CIO Ratings (Risk Management Assessment)

In accordance with Executive Order 13800, OMB, in coordination with DHS, developed a process to evaluate the degree to which agencies manage their cybersecurity risk at the enterprise level. Since the publication of this memo, the Risk Management Assessments (RMAs) continue to evolve in order to meet the ever-changing nature of the Federal cybersecurity risk environment.

The risk assessments leverage the FY 2018 FISMA CIO Metrics in domains that correspond with the NIST Cybersecurity Framework:

- **Identify** (Asset Management; System Authorization)
- **Protect** (Remote Access Protection; Credentialing and Authorization; Configuration and Vulnerability Management; HVA Protection)

[57] 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.

[58] 44 USC § 3555(b)(2) agencies that do not have 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.

- **Detect** (Intrusion Detection and Prevention; Exfiltration and Enhanced Defenses)
- **Respond and Recover**[59]

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.

IG Ratings

Independent assessors, most often agency IGs, evaluate each agency's information security program and provide ratings based on a maturity model with five levels, as described in FY 2018 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

Table 14 provides the median maturity model ratings across the five NIST Cybersecurity Framework functions from 84 agency IG and independent auditor assessments. Notably the median Detect framework function rating improved from *Defined* (Level 2) in FY 2017 to *Consistently Implemented* (Level 3) in FY 2018.

[59] 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

Table 14 IG Assessment Maturity Levels

NIST Cybersecurity Framework Function	Median Rating
Identify	*Consistently Implemented*
Protect	*Consistently Implemented*
Detect	*Consistently Implemented*
Respond	*Consistently Implemented*
Recover	*Consistently Implemented*

Per the IG Reporting Metrics, a finding of *Managed and Measureable* (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 FY 2018 IG FISMA Metrics provide IGs with the discretion to rate their agencies as effective below the *Managed and Measureable* level. However, OMB strongly encouraged IGs to rely on the performance metrics to determine the effectiveness of their agencies' cybersecurity programs.

Government-wide Cybersecurity Cross-Agency Priority (CAP) Goal Performance

The President's Management Agenda (PMA) lays out a long-term vision for modernizing the Federal Government. To drive management priorities, the Administration leverages Cross-Agency Priority (CAP) Goals to coordinate and publicly track implementation across Federal agencies.

Cybersecurity remains a priority for the Administration, and its integration into the *Modernize IT to Increase Productivity and Security* CAP Goal demonstrates the Administration's view that cybersecurity is inseparable from broader Federal IT policy. This CAP Goal captures not only progress on implementing key security controls and capabilities, but also the status of larger efforts to change how the Federal Government approaches both information security and IT more generally. A summary of the Federal Government's overall performance on these key cybersecurity metrics can be found below in Table 15. For more information on this CAP Goal, see Performance.gov.

Table 15 FY 2017 - FY 2018 CAP Goal Summary

CAP Goal Metric	Target	Number of Agencies Meeting Target		Average Implementation*	
		FY 2017	FY 2018	FY 2017	FY 2018
Manage Asset Security					
Hardware Asset Management	95%	58	71	67%**	64%**
Software Asset Management	95%	53	56	69%**	58%**
Authorization Management	100%	51	79***	84%	91%
Mobile Asset Management	95%	N/A	78	N/A	96%
Limit Personnel Access					
Privileged Network Access Management	100%	46	56	93%	94%
High Value Asset System Access Management	90%	N/A	58***	N/A	70%
Automated Access Management	95%	N/A	63	N/A	63%
Protect Networks and Data					
Intrusion Detection and Prevention	4 of 6	N/A	45	N/A	N/A
Exfiltration and Enhanced Defenses	3 of 4	N/A	93	N/A	N/A
Data Protection	3 of 6	N/A	67***	N/A	N/A

Source: Metrics as described in Appendix A of FY 2018 FISMA CIO Metrics
* OMB used a weighted average of applicable assets or users to determine the government-wide average
** July 2018 changes to CIO Metrics added the requirement that whitelisting capabilities be "centrally visible at the enterprise-level"
*** 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

B. FY 2018 Information Security Incidents[60]

US-CERT Incidents by Attack Vector[61]

Agency incident data provides an indication of the threats agencies face every day and the persistence of those incidents. In accordance with FISMA, OMB collects summary information on the number of cybersecurity incidents that occurred across the Federal Government and at each Federal agency to better understand and oversee the threat landscape. The FY 2018 FISMA Report captures incidents in accordance with US-CERT's revised Incident Notification Guidelines, which require agencies to use an incident reporting methodology that classifies incidents by the method of attack, known as attack vector, and to specify the impact to the agency.[62]

Table 16 highlights 31,107 incidents reported by Federal agencies, and validated with US-CERT, across nine attack vector categories. This represents a 12% decrease from FY 2017, when agencies reported 35,277 incidents. While the trend is encouraging, drawing conclusions based on this data point, particularly as agencies have adjusted to several new sets of reporting guidelines over the last few years, would be concerning. As noted earlier, email-based threats remain prevalent, with Email/Phishing continuing to be a highly-targeted attack vector. According to information provided by DHS, 6,930 incidents occurring in the past year. Moreover, nearly 27% of all incidents did not have an identified attack vector, which continues to suggest that the government must take additional steps to help agencies identify the sources and vectors of these incidents.

[60] See Appendix I for additional information about the definition and reporting requirements for major incidents.
[61] 44 USC § 3553(c)(1).
[62] 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 16 Agency-Reported Incidents by Attack Vector

Attack Vector	FY 2017 CFO	FY 2017 Non-CFO	FY 2017 Gov-wide	FY 2018 CFO	FY 2018 Non-CFO	FY 2018 Gov-wide
Attrition An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	148	3	151	149	14	163
E-mail/Phishing An attack executed via an email message or attachment.	6,918	410	7,328	6,423	507	6,930
External/Removable Media An attack executed from removable media or a peripheral device.	71	1	72	32	0	32
Impersonation/Spoofing An attack involving replacement of legitimate content/services with a malicious substitute.	N/A	N/A	N/A	44	3	47
Improper Usage Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	7,575	281	7,856	9,315	359	9,674
Loss or Theft of Equipment The loss or theft of a computing device or media used by the organization.	4,102	293	4,395	2,236	316	2,552
Web An attack executed from a website or web-based application.	3,922	127	4,049	3,242	90	3,332
Other / Unknown An attack method does not fit into any other vector or cause of attack is unidentified.	10,169	656	10,825	7,942	343	8,285
Multiple Attack Vectors An attack that uses two or more of the above vectors in combination.	579	22	601	90	2	92
Total	**33,484**	**1,793**	**35,277**	**29,473**	**1,634**	**31,107**

C. Agency Cybersecurity Performance Summaries

FY 2018 Annual Cybersecurity Performance Summary

Advisory Council on Historic Preservation

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

In FY18 the ACHP has taken several steps to significantly improve cybersecurity capabilities and protect the integrity of agency systems, HVAs, and mission functions. The agency was able to put into production automated scanning of vulnerabilities which improved patching workflow; monitoring of netflow traffic for security incidents; monitoring of all credentialed login attempts for on-premise and cloud systems; integrated APT, malware protection and threat correlation; and SIEM deployment to provide integrated views and alerting of incidents.

Security program reviews have demonstrated progress this year in improvement of security posture, and integration of tools that greatly improve cybersecurity incident monitoring, prevention, and response in subsequent quarters. However, implementation of multi-factor AAL3 authentication, data at rest encryption, off-site replication and HVA patching is constrained due to lack of resources at the moment. DMARC resolution should be resolved by year's end; HVA patching is anticipated to be conducted in Q1 2019 after the maintenance contract is funded.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Advisory Council on Historic Preservation was not performed for FY 2018, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Advisory Council on Historic Preservation will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

African Development Foundation

Framework	CIO Rating	IG Rating
Identify	At Risk	Defined
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	2	0
Multiple Attack Vectors	0	0	0
Total	0	2	0

CIO Self-Assessment

The United States African Development Foundation (USADF} has developed a risk management governance that is demonstrated through the implementation and maintenance of a risk management structure that addresses the organization-wide risk management strategy. USADF strives to mitigate cybersecurity risks by implementing through its leadership an organization-wide enterprise risk management plan, remaining compliant by participating in the DHS's CDM program. USADF performs an annual security and risk assessment on its information system resources according to the National Institute of Standards and Technology Standard Publication guidelines and in compliance with the Federal Information Security Modernization Act of 2014. USADF has equally outsourced cybersecurity risks by moving critical assets to US government shared services and to FedRAMP approved cloud services providers. USADF has implemented DHS mandated EINSTEIN 3A IPSS DNS and IPSS Cloud Email as part of its effort to mitigate and reduce cybersecurity risk exposure. Even though the Foundation has enamored these efforts in managing risks, challenges still exist.

USADF, from a risk management strategy perspective, has implemented a Risk Management Plan that covers risk management of all the Foundation's information system resources internally or externally hosted and managed. Information system resources are categorized based on the business function, threat exposure; vulnerabilities and data type pursuant to the System Security Plan {SSP). Strategies for risk remediation are proportionate to the risks to the information system resources. Selected and implemented risk management measures reasonably protect the confidentiality, integrity and availability of information system resources and the risk is managed continuously.

Independent Assessment

The information security program of the African Development Foundation was evaluated as effective. The audit noted that 46 of 59 selected NIST SP 800-53, Revision 4, security controls were properly implemented. This led to the determination of USADF having an overall effective information security program. There were three recommendations made to help USADF improve their information security program.

FY 2018 Annual Cybersecurity Performance Summary

American Battle Monuments Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	0	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	3	2	1
Multiple Attack Vectors	0	1	0
Total	4	3	3

CIO Self-Assessment

The commission recently engaged consulting professionals to help the Agency assess, review and enhance its IT organization, roles, processes and governance. This led to defining a full-time CIO position to spearhead the Agency IT modernization efforts.

Furthermore, the following steps were taken during FY18:

- Recruiting two IT Specialists with Cybersecurity and Information Assurance experience.
- Engaging in the DHS CDM program.
- Deploying DHS Einstein3A service covering web and email traffic.
- Multiplying cybersecurity training and education opportunities for all employees and account holders agency-wide.
- Committing in the DHS Cyber Hygiene Program as well as aggressively tackling Binding Operational Directive milestones.

Independent Assessment

The information security program of the American Battle Monuments Commission was evaluated as effective. ABMC does not have an Inspector General, therefore an independent certified accounting firm was contracted to perform the assessment.

The scope of the assessment included all aspects of ABMC's IT environment. Overall ABMC's information security program is effective, but can be improved upon. The current year state of ABMC's information security program significantly changed from the prior year due to a significant organizational change. All of the assessment areas were significantly impacted and new policies and procedures need to be put in place. The organizational change, coupled with the geographic dispersion of its operations has continued to impact ABMCs overall assessment.

OIG primary recommendations are for ABMC to update POAMs and CAP Goals based on the organizational change and to ensure its information technology environment and infrastructure is part of their annual enterprise risk management process.

In FY18 ABMC IT hired three additional IT personnel, one cybersecurity professional in their overseas operations and two IT security specialists at HQ. Additionally, in FY18 ABMC undertook a CIO study to determine the need of a dedicated full time CIO. The study resulted in the recommendation to hire a CIO and at this time the position has been advertised and the position should be filled in FY19.

FY 2018 Annual Cybersecurity Performance Summary

Armed Forces Retirement Home

Framework	CIO Rating	IG Rating
Identify	At Risk	Consistently Implemented
Protect	At Risk	Managed and Measurable
Detect	At Risk	Defined
Respond	Managing Risk	Managed and Measurable
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The AFRH has made great progress towards implementing measures to protect its IT assets, environment and mission critical functions from cyber attacks. The AFRH contracts with the Department of Interior's OCIO through an inter-agency agreement (IAA), for hosting, website, network and MTIPS support. AFRH's Information Technology infrastructure during FY 2018 has improved significantly over its previous year's report.

A POA&M is developed and remediated based upon the identified risks found during the SSA and an annual self-assessment process. As AFRH continues to ensure that it complies with NIST and FISMA standards, a strong emphasis has been placed on our security programs, with the understanding that constant monitoring for improvements and changes implemented based on factors in the environment and industry are key to preventing security weaknesses and cyber attacks.

The AFRH will continue its IAA with the DOI's OCIO to implement an aggressive ISCM process during FY 2019, which provides daily, weekly and monthly reports to the DOI OCIO customer base in a secure location for review. This process has been firmly linked to the monitoring by the DHS US-CERT Office to ensure rapid incident reporting. The AFRH prides itself on using public resource partners who understand the importance of federal security and who are familiar with FISMA requirements and NIST standards to ensure that the AFRH continues to operate in a solid and robust security framework.

Independent Assessment

The information security program of the Armed Forces Retirement Home was evaluated as effective. AFRH uses an integrative approach to manage risks for information security, through strategic planning, reviews, internal control activities, reporting and monitoring in alignment with AFRH's strategic mission. In coordination with DOI OCIO, AFRH continues to make strides in documenting, validating, measuring and implementing continuous monitoring of security processes and procedures across its IT Security Program. AFRH has seen major improvements in Incident Response, defining the CP Process, Configuration Management and overall Risk management for AFRH IT Systems and data centers with a concerted effort by all parties involved.

There are still some identified deficiencies in the areas such as automation of risk management, consistent contingency planning exercises and multifactor authentication implementation that are being reviewed for implementation and improvement.

FY 2018 Annual Cybersecurity Performance Summary

Board of Governors of the Federal Reserve

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	1
E-mail	1	1	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	1	0
Loss or Theft of Equipment	0	0	0
Web	3	0	0
Other	4	5	1
Multiple Attack Vectors	0	0	0
Total	9	7	2

CIO Self-Assessment

Primary cybersecurity risks to the Federal Reserve Board's (Board), including its HVA and MEF, are phishing emails carrying advanced malware; ransomware and distributed denial-of-service (DDoS) attacks that target the availability of data and systems; and trusted insiders with access to sensitive data.

Prior to 2018, the Board had already deployed a layered approach to addressing these risks:

- Layered perimeter security that includes, web content filtering, intrusion prevention, email filtering, Einstein 3A monitoring services, and Data Loss Protection (DLP);
- Next generation endpoint and network based security to decrease our exposure to zero-day attacks;
- Enforcement of two-factor PIV authentication for privileged users;
- Anti-DDOS protections;
- High availability configurations of high value assets;
- Conducting network monitoring for anomalies and suspicious activity;
- Conducting end-user security awareness training to include phishing awareness simulations to ensure that users are aware of real-world phishing attack methods and the risks associated with these attacks.
- Multiple third party assessments beyond the work done by the Office of Inspector General.

In 2018, the Board has completed multiple projects to further enhance our protections:

- Completed implementation of two-factor PIV authentication for all users
- Enhanced monitoring of user behavior
- Initiated a review of DDOS protections

Independent Assessment

The information security program of the Board of Governors of the Federal Reserve was evaluated as effective. The OIG found that the Board's information security program includes policies and procedures that are generally consistent with the functional areas outlined in the NIST Cybersecurity Framework. However, we identified opportunities to strengthen processes and controls in the areas of risk management, configuration management, data protection and privacy, and security training to further mature the program and ensure that it remains effective. The OIG audit report includes 6 recommendations to strengthen controls in these areas.

FY 2018 Annual Cybersecurity Performance Summary

U.S. Agency for Global Media (formerly Broadcasting Board of Governors)

Framework	CIO Rating	IG Rating
Identify	At Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	At Risk	Ad Hoc
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	0	2
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	0	5	0
Other	7	7	2
Multiple Attack Vectors	0	0	0
Total	8	12	5

CIO Self-Assessment

Over the past year, USAGM has acted to bolster our information security and risk management posture and lay the framework for systemic improvements in risk management. The Agency has appointed a Chief Risk Officer (CRO) to lead the design, development, and implementation of the agency's ERM program. The CRO has already led USAGM through a risk identification process, and he and his team are busy assessing prioritizing the identified agency-wide risks, including IT risks, to the agency's strategic objectives. Over the next few months, USAGM will continue the ERM process to develop its first risk profile. Results of this work will be submitted for approval to USAGM's new Risk Management Council, made of up the agency's senior leadership.

The CRO is working closely with the agency's CIO and CISO to ensure that information security risks are embedded in USAGM's overall risk profile. The CRO will also work closely with our CIO's staff to further develop their IT risk management strategy to make sure that it aligns with the NIST guidance and to make sure IT-related risks are included in every stage of the ERM process.

USAGM has carefully designed and documented its updated delegation of authority to the CIO issued early in 2018, as well as the governance structure for its ERM program and CIO Council. The CIO Council, chaired by the CIO and attended by CIOs or equivalent representatives from USAGM's broadcast entities, adopted a CIO Council Charter, which establishes a framework under which the CIO Council members can work collaboratively to safeguard federal and non-federal information assets that support the USAGM mission.

Independent Assessment

Acting on behalf of the Office of Inspector General, an independent assessor conducted this audit to determine the effectiveness of the USAGM's information security program and practices in accordance with FISMA requirements in FY 2018. The independent assessor concludes that the USAGM does not have an effective organization-wide information security program for several reasons. OIG made six recommendations to improve USAGM's information security program.

FY 2018 Annual Cybersecurity Performance Summary

Chemical Safety Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The agency's overall cybersecurity and information security program is effective. All agency internet traffic is subject to continuous monitoring. Traffic between Headquarters and the Western Regional Office is encrypted in a LAN-to-LAN tunnel, and remote access is encrypted through VPN client connections to the same firewalls. User traffic is monitored in both locations by email and web filter appliances with continually updated definitions. All machines are protected by centrally managed anti-virus and antimalware. Mobile devices are protected by a centrally managed mobile device management solution, and email is protected through an email gateway appliance along with anti-spam and anti-phishing software. Internet and email traffic pass through a Verizon MTIPS connection and the DHS E3A gateway.

Independent Assessment

The information security program of the Chemical Safety Board was evaluated as effective. CSB has demonstrated it has defined policy, procedures and strategies for all five of the information security function areas. The OIG assessed the five Cybersecurity Framework function areas in adherence to the FY 2018 IG FISMA reporting metrics. If the policies, procedures and strategies were formalized and documented the agency was rated at level 2 (Defined). If not, the OIG rated the agency at level 1 (Ad Hoc). Several areas within the CSB's information security program were identified at level 1 (Ad Hoc). Based on our analysis, improvements are needed in the following areas:

- Identity and Access Management: CSB does not include fully defined processes for Personal Identity Verification card technology for physical and logical access.
- Incident Response: CSB has not identified nor fully defined its incident response processes.

FY 2018 Annual Cybersecurity Performance Summary

Commission of Fine Arts

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	High Risk	NA
Detect	At Risk	NA
Respond	Managing Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	2	0
Other	0	0	0
Multiple Attack Vectors	0	2	0
Total	0	0	0

CIO Self-Assessment

The most significant cybersecurity risk to the Commission of Fine Arts (CFA) is the absence of knowledgeable and dedicated IT and cybersecurity staff, or access to such staff elsewhere, with the capacity and expertise to fully address the CFA's cybersecurity infrastructure. However, the CFA endeavors to manage and mitigate risks to the best of its capacity.

Efforts to improve the cybersecurity posture this past year include engaging a more reliable vendor for Malicious Email Filtering MEF functions, participation in the DHS's CDM initiative and the initial implementation of tasks within BOD 18-01. The CFA declared that its GSS is not considered a HVA as defined in BOD 18-02, due to its small scope and levels of redundancy. The CFA staff received ad-hoc training in phishing attempts and are become adept at recognizing such attempts.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Commission of Fine Arts was not performed for FY 2018, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Commission of Fine Arts will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Commission on Civil Rights

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	At Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	0	0
Multiple Attack Vectors	0	0	0
Total	2	0	0

CIO Self-Assessment

The United States Commission on Civil Rights (USCCR) risk assessment of its information and information systems included risks to the Agency's High Value Assets, Mission Essential Functions, and level and program specific security reviews. USCCR evaluated three elements from its master risk register to include risk probability, impact, and exposure. The Commission assessed the likelihood of risk, inventoried IT systems and data to create an individualized list of the risk's impact to each system, and performed a risk analysis of each system. This allowed the Agency to identify vulnerabilities for management in order to develop a risk mitigation strategy for operations staff and contractors to appropriately prioritize and manage risks.

USCCR planning activities are carried out by the Agency's IT security and operations teams, which enables staff to prioritize the risks and develop mitigation strategies.

USCCR management aims to have all risks mitigated on time and on budget; however, certain risks are unable to be fully resolved due to budget, personnel, resources, and processes.

USCCR management must be strategic in decisions due to a limited operational budget. Therefore, the agency prioritizes what risks it mitigates, transfers, or accepts according to its resources. The Agency is forced to accept some risks based on the likelihood of occurrence, impact of exploitation, and cost of implementation. The decisions on the Agency's risk strategies are documented, tracked, and managed according to the Agency's risk management policy. The risk assessment revealed gaps across all of the NIST Framework Functions and domains. The Commission plans to address them soon and track the areas through a Plan of Action and Milestones in order to improve the security posture of the agency. USCCR senior leaders stay apprised of risk within the enterprise by receiving monthly briefings on vulnerability mitigation plans and actions being taking to improve the agency's cybersecurity posture.

Independent Assessment

The information security program of the Commission on Civil Rights was evaluated as effective. To meet FISMA requirements with respect to the US Commission on Civil Rights, the agency contracted with an independent auditor to conduct the FY 2018 independent evaluation of USCCR's information security program and practices as a performance audit under Generally Accepted Government Auditing Standards. The auditors for USCCR concluded that overall, United States Commission on Civil Rights (USCCR) has invested significantly to ensure that its information security policies and procedures comply with FISMA requirements and recommendations made over the past year.

The agency has developed several POA&Ms to address FISMA requirements. The scope of the evaluation included all aspects of USCCR's IT environment. Overall USCCR's information security program is effective, but can be improved upon. The primary reason for the "consistently implemented" state of USCCR's information security program is based on weaknesses found in the areas of Identify, Protect, and Respond. The state would have "managed and measurable if the agency was to obtain the resources to fully implement the security program. The primary recommendation is to address the POA&Ms already identified and to ensure that the policies and procedures outlined in the POA&Ms is successfully addressed in FY2019.

FY 2018 Annual Cybersecurity Performance Summary

Commodity Futures Trading Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	0
E-mail	0	1	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	1	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	2	2
Multiple Attack Vectors	0	0	0
Total	2	5	3

CIO Self-Assessment

CFTC has built an Enterprise Information Security Program to address the constantly growing threat landscape, with a balanced mix of policy and compliance activities to govern the protection of our assets and mission functions.

Recently identified risks include residual weaknesses related to internal controls; specifically, access controls, continuous monitoring controls, and boundary protection practices designed to protect mission essential functions. The Commission also needs to improve on the timely remediation of those persistent security vulnerabilities on our infrastructure. Efforts should focus on establishing effective processes to ensure timely corrective actions are implemented on outstanding system security risks as documented in the POAMs.

Protecting HVAs and Mission Essential Functions also requires capabilities and resources that are not yet in place, including an Insider Threat Program, automated tools and predictive and preventative technologies. We will reevaluate and further define our high value assets in FY19.

Key gaps that have been identified in our information security program include:
• Fulfillment of DHS CDM program dependencies
• Timely remediation of POAMs on major systems
• Role-based security training to FISMA mandatory roles
• Full compliance with CAP goal PIV usage
• Development of an insider threat program to include DLP capability
• GRC policy enforcement
• Establish ERM Program

The impacts of added requirements from the cybersecurity legislation, our understanding of the threat landscape, and the constant evolving practices of information security, require that we carefully examine the effects and apply best practices how to provide timely, reliable, and secure IT services.

Independent Assessment

The information security program of the Commodity Futures Trading Commission was evaluated as effective.

While CFTC's IT security program is rated effective overall, there are opportunities to optimize the program. We recommend CFTC:

1) Leverage next generation program tools to enhance network scanning capabilities and develop a continuous comprehensive inventory;
2) Improve logical access account management and monitoring of legacy systems hosting market data;
3) Mature an Enterprise Architecture program (reported separately); and
4) Continue to mature insider threat and enterprise risk management programs (open recommendations from FY 2017).

Consumer Financial Protection Bureau

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	5	3	3
Loss or Theft of Equipment	108	120	151
Web	15	6	0
Other	22	13	10
Multiple Attack Vectors	1	2	0
Total	152	146	164

CIO Self-Assessment

Since the Bureau was established in 2011, the BCFP has taken an innovative approach to fulfill its mission to serve the American consumer by becoming a cloud-first agency that leverages digital technologies. While this approach to become a modern agency presents opportunities for efficiency and innovative services, it does not come without challenges. The BCFP uses internal security controls assessments, continuous monitoring, and audits to identify cybersecurity risks and opportunities to gain efficiencies in operations that enhance overall mission effectiveness. The results of these activities are further analyzed to help inform decisions that consider the following:

- Achieving and maintaining visibility into the data and assets that need to be protected in a distributed IT environment that embraces the shared service models of FedRAMP and federal service providers;
- Addressing the data protection needs of the organization focused on the Bureau's high value assets (HVAs), while not hindering BCFP's ability to interface with the public or limiting the Bureau's mission to ensure fairness in the financial marketplace and improve financial education and awareness;
- Achieving near real-time situational awareness to cyber threats and vulnerabilities;
- Safeguarding sensitive information from misuse or alteration, while also making the appropriate data available to carry out the BCFP's mission.

During its formation, the BCFP seized the opportunity to establish a cost-effective, risk-based strategy to implement the NIST Risk Management Framework (RMF) and manage cybersecurity risks. As pressure from check-box compliance activities increased, the priority shifted to address Bureau functions subject to audits. Beginning late 2016 and continuing into 2018, the BCFP has re-centered on a risk-based approach that employs the RMF and aligns to the Cybersecurity Framework to identify and manage risk to its high value assets, thereby evolving the enterprise-wide view of risk.

Independent Assessment

The information security program of the Consumer Financial Protection Bureau was evaluated as not effective. Overall, we found that the Bureau's information security program is operating at a level 3 (consistently implemented). We also found that the Bureau's information security program includes policies and procedures that are generally consistent with the function areas outlined in the NIST Cybersecurity Framework. However, we identified opportunities to strengthen processes and controls in the areas of configuration management, identity and access management, and data protection and privacy to further mature the program and ensure that it is effective. Our audit report includes 4 recommendations to strengthen controls in these areas.

FY 2018 Annual Cybersecurity Performance Summary

Consumer Product Safety Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Managed and Measurable
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	0
E-mail	2	4	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	1	0
Loss or Theft of Equipment	0	0	5
Web	3	2	0
Other	5	7	2
Multiple Attack Vectors	0	0	0
Total	10	15	8

CIO Self-Assessment

CPSC continues to make progress in improving its information security posture. During FY 2018, the agency conducted independent assessments of its major information systems—which showed a 67% reduction in findings compared to FY 2017. The CPSC's Office of the Inspector General (OIG) FISMA Review for FY 2018 identified 17 findings. Although this is an increase of three from our FY 2017 report, this does not indicate a deterioration of our program nor of our commitment to security and privacy, but rather reflects an increase in the level of maturity that our programs are being assessed.

The following items describe the Cybersecurity risks--related to the agency's High Value Asset and Mission Essential Functions--that the agency is currently facing:

1) The agency does not currently meet the CAP goal target for enforcement of two-factor PIV authentication for privileged network access. CPSC intends to address this gap in FY 2019. CPSC has procured the DHS Continuous Diagnostics and Monitoring (CDM) access management solution to fill this gap in FY 2018 and is in the process of full implementation.
2) The agency does not currently have an automated capability to block and alert when an unauthorized device is connected to the agency's network. This will be addressed through the planned activity for the implementation of a NAC system.
3) The agency does not consistently remediate discovered vulnerabilities in critical IT components within the timeframes required by agency policy. This will be addressed through the planned activity relating to the implementation of an automated patch management process.
4) The agency does not consistently implement secure configurations for critical IT components. The agency intends to formalize this aspect of its configuration management practices to include documentation of approved deviations from standard configurations.

Independent Assessment

The information security program of the Consumer Product Safety Commission was evaluated as not effective. CPSC improved its policies and procedures, implemented new cybersecurity solutions, and is actively working toward standardizing its risk documentation.

CPSC has not: developed and maintained a comprehensive software and hardware inventory; documented and implemented baseline configurations for all agency hardware and software; applied patches in a timely manner; enforced multi-factor authentication; properly applied the Principle of Least Access; developed and maintained a business impact assessment and contingency and continuity plans; provided role-based security and privacy training to all applicable agency resources; implemented an organization-wide risk management program; or implemented processes to adequately protect PII throughout the data lifecycle. IT contracts and agreements for goods and services lack required Federal Acquisition Regulation clauses and/or other provisions.

Corporation for National and Community Service

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Consistently Implemented
Detect	At Risk	Defined
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	4	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	0	1
Loss or Theft of Equipment	14	4	1
Web	1	1	0
Other	5	6	0
Multiple Attack Vectors	0	0	0
Total	25	13	2

CIO Self-Assessment

CNCS directly manages six information systems that are under an ongoing authorization. To maintain ongoing authorization CNCS reviews predefined sets of NIST SP 800-53 security controls each month to ensure systems are operating securely and effectively. Continuously looking at each information system has decreased the number of non-compliant security controls and increased the effectiveness of those controls. Each information system in FY 2018 has received an annual security assessment that reviews/test significant security controls that offer a high level of assurance about the overall security of the information system as well as any controls that did not pass the monthly review.

As a result of the Office of Information Technology (OIT) efforts to improve security and completion of the required annual FISMA assessment, CNCS understands that its information system security program is operating in an AT RISK state. CNCS has assessed that this level of risk is due to a legacy High Value Asset (HVA) requiring software and hardware updates; the lack of automated centralized reporting of hardware and software; and the lack of identity management.

To remediate these risks CNCS will upgrade the HVA system to remediate vulnerabilities, continue coordination with the DHS to implement a CDM program and implement multifactor authentication to directly manage identity access control. Planning for each of these projects was completed in FY 2018 with the implementation scheduled for completion by the end of FY 2019.

Independent Assessment

The information security program of the Corporation for National and Community Service was evaluated as not effective. The OIG determined through independent review that the agency does not have an effective information security program. While the Corporation has devoted significant resources to improving its information security program and practices over the past few years, those efforts have focused on developing policies and procedures and system security documentation. These are necessary and foundational, but they are of limited value unless they are supported by consistent implementation and monitoring of security controls. Overall, the Corporation made small gains in certain components of the objective metrics, but those improvements did not move CNCS's information security program substantially closer to an Effective level, especially relative to the resources invested.

The independent IG report offers 24 recommendations to assist CNCS in strengthening its information security program including recommendations to assist CNCS to reach an Effective rating. The recommendations are focused on the review of the Corporation's weaknesses and the IG Metrics questions; the goal is to better strategically plan, prioritize and allocate CNCS resources to implement steady measurable multi-year improvements towards an effective risk based information security program.

FY 2018 Annual Cybersecurity Performance Summary

Council of the Inspectors General on Integrity and Efficiency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	0	0	1

CIO Self-Assessment

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) relies on cloud-based service providers to perform most of its critical functions, and maintains a GSS that provides employees with secure access to the internet, data storage, computational resources and interconnectivity between our two locations.

CIGIE continues to improve its information security posture to ensure that the CIGIE GSS meets federal mandates and NIST recommendations. CIGIE is continuously identifying and mitigating any potential risks to the GSS through enhancement and modernization of perimeter controls. Furthermore, CIGIE is adopting Government best practices for cybersecurity management and protection controls including single sign-on, advanced monitoring tools, high-availability and mobile technologies.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Council of the Inspectors General on Integrity and Efficiency was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Council of the Inspectors General on Integrity and Efficiency will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Court Services and Offender Supervision Agency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Defined
Detect	Managing Risk	Ad Hoc
Respond	Managing Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	3
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	1
Web	0	1	0
Other	0	4	1
Multiple Attack Vectors	0	0	0
Total	0	5	5

CIO Self-Assessment

Cybersecurity continues to be one of the Administration's top priorities. In conjunction with OMB and DHS, CSOSA is accelerating its activity around protecting the mission from a cybersecurity perspective. The Agency is focused on strengthening its security posture and defending against attacks on sensitive law enforcement, national security, and U.S. government personnel data, while maintaining the confidentiality, integrity, and availability of mission systems. The Agency has made significant progress in managing information risk and securing our systems, and must continually invest in our cybersecurity capabilities to be effective.

Independent Assessment

The information security program of the Court Services and Offender Supervision Agency was evaluated as not effective. Overall, the Agency (CSOSA and PSA) has made progress in addressing previously identified information security deficiencies.

FY 2018 Annual Cybersecurity Performance Summary

Defense Nuclear Facilities Safety Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	2
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	0	2	2

CIO Self-Assessment

DNFSB engaged a third party contractor to perform an Independent Network Risk and Vulnerability Assessment. The assessment entailed a documentation review against federal requirements, a GSS scan for vulnerabilities, external penetration testing, and a social engineering campaign. The external penetration testing found no major issues and all findings carried a low or informational risk level. The implementation of Varonis Insider Threat Detection software on the GSS reduced the deficiency in the Detect control. The agency is implementing the assessment analysis and findings to continue to enhance the current strengths of the cybersecurity program.

Independent Assessment

The information security program of the Defense Nuclear Facilities Safety Board was evaluated as effective. Due to the small organizational structure, DNFSB has the ability to operate and communicate more efficiently and effectively compared to larger Federal agencies. DNFSB's key risk management personnel are intimately involved in all aspects of DNFSB's risk management, configuration management, ICAM, data protection and privacy, ISCM, incident response, and contingency planning programs and are aware of every important decision involving its IT operations and above-mentioned programs. However, DNFSB has not fully developed and implemented policies and procedures in many of its programs. In order to mature its programs, DNFSB should continue to develop and implement policies and procedures in programs that lack policies and procedures and make improvements to existing policies and procedures.

FY 2018 Annual Cybersecurity Performance Summary

Denali Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	At Risk	Ad Hoc
Respond	High Risk	Ad Hoc
Recover		Ad Hoc
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Denali Commission (Denali) does not collect PII and systems collecting private data are not housed at the Agency. Denali is a relatively small agency that relies upon the shared services provider, Bureau of Fiscal Services (Treasury), to provide much of their IT security. Denali does not have any HVAs.

Independent Assessment

The information security program of the Denali Commission was evaluated as not effective. Denali Commission uses the United States Treasury Shared Services systems. In past years, due to the small size of the agency, much of the NIST Cybersecurity Framework was not applicable to Denali because the information was not kept within their network. Denali's information security program does not have fully documented and sufficient policies and procedures to identify, protect, detect, respond, and recover components of the NIST Cybersecurity Framework. Although the information security program could use improvement, the Agency is still at a relatively low risk of encountering cyber attacks due to the amount and type of information stored within its network.

FY 2018 Annual Cybersecurity Performance Summary

Department of Agriculture

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	4	0	1
E-mail	27	40	20
External/Removable Media	1	0	1
Impersonation	3	NA	0
Improper Usage	293	413	323
Loss or Theft of Equipment	155	182	9
Web	381	226	161
Other	962	464	365
Multiple Attack Vectors	41	43	49
Total	1,867	1,368	929

CIO Self-Assessment

In compliance with EO 13800 and OMB M-17-25, the Department of Agriculture (USDA) has established Cybersecurity operations that directly correlate to the capabilities outlined in the NIST Cybersecurity Framework. USDA has prioritized implementing corrective actions in control areas identified in the CIO FISMA Risk Management Assessment as “High Risk” and “At Risk” to achieve “Managing Risk”.

In compliance with BOD 18-02 USDA has focused resources to ensure implementation of critical cybersecurity controls on its HVAs. Additionally, we are actively engaged with DHS to conduct ongoing RVAs and SARs on USDA HVA systems consistent with BOD 16-01. USDA receives weekly cyber hygiene reports from DHS on our enterprise environment and immediately coordinates corrective actions on identified vulnerabilities with our subcomponent system owners.

The USDA has aligned the Cyber Security Strategic Plan to the USDA’s overall Strategic Business Plan and works enterprise-wide to implement these strategic plans. USDA has implemented a strong IT Risk Management framework to identify and manage cyber security risks to systems, assets, data, and capabilities. The program begins at the investment level and follows through to the day-to-day implementation of Cyber Security controls and continuous monitoring across the Department. USDA integrates appropriate safeguards to protect and limit the impact of cyber security events using controls outlined by NIST 800-53, OMB and other federal regulations.

Independent Assessment

The information security program of the Department of Agriculture was evaluated as not effective. The Department took some positive steps to improve the Department’s security posture in FY 2018. For example, a significant improvement was made to the risk management program by reducing the number of systems operating without ATOs. However, improvements are still needed for many functions. The Department consistently issues policies that delegate procedures and responsibilities for compliance to the agencies. In spite of available tracking mechanisms, Department scorecards, and tools such as CSAM, the results of the audit demonstrated that the Department did not have necessary assessment and/or enforcement processes in place to ensure agency compliance. As with the Department consolidation of the workstations management, we encourage the Department to continue to consolidate common IT functions into a central corporate model and improve the oversight of the agencies’ compliance with Department policies.

FY 2018 Annual Cybersecurity Performance Summary

Department of Commerce

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	5	15	4
E-mail	346	567	660
External/Removable Media	5	1	0
Impersonation	3	NA	2
Improper Usage	175	407	582
Loss or Theft of Equipment	87	131	67
Web	232	210	196
Other	1,528	655	305
Multiple Attack Vectors	194	21	11
Total	2,575	2,007	1,827

CIO Self-Assessment

In FY18, the primary cybersecurity risks facing the Department were: a lack of real time continuous monitoring capabilities to facilitate standardized risk-based information security management; deficiencies in identifying and mitigating vulnerabilities expeditiously; a continued inability to attract, hire, and retain staff needed to maintain security processes on DOC systems and environments; and a lack of enhanced security controls required for HVA systems.

To mitigate these risks, the Department continued to implement and mature multiple enterprise-wide initiatives including the phased deployment of the CDM program, for which a contract for Phase 3 DEFEND was recently awarded, and collaborate with the Department's sub-components on supplemental scanning, monitoring, and patching capabilities. Additional improvements to monitoring and incident response capabilities are expected as the Department continues to expand the integration of the Enterprise Continuous Monitoring Operations (ECMO) program to high impact systems, and to expand Enterprise Security Operations Center (ESOC) capabilities, supplementing them with tools made available through the CDM Program.

In response to guidance from the Office of Personnel Management the Department also began to code its cybersecurity positions to identify and address critical staffing gaps. It plans to maximize the use of direct hiring authorities for cybersecurity positions. The Department continues to work with its sub-components that operate HVA systems to identify solutions to implement heightened security controls, mitigate risks that are present in the interim, and document the Plans of Actions and Milestones (POA&Ms) to mitigate risks accordingly in the Department's POA&M and inventory tracking system Cyber Security Assessment Management (CSAM) tool.

Independent Assessment

The information security program of the Department of Commerce was evaluated as not effective. The OIG completed an audit of Commerce's FISMA compliance by assessing the effectiveness of Commerce's information security program and practices. OIG also reviewed a representative subset of 15 IT systems from 5 of Commerce's operating units to assess compliance.

OIG's assessments of the five functional areas (Identify, Protect, Detect, Respond, and Recover) found that the Department had largely defined needed policies and procedures. We also found that, in general, the metrics related to security training, information security continuous monitoring, and incident response were managed and measurable. However, we found that the Department did not consistently implement IT security procedures and practices in risk management, configuration management, identity credential and access management, data protection and privacy, and contingency planning.

FY 2018 Annual Cybersecurity Performance Summary

Department of Education

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover	Managing Risk	Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	1	0	2
E-mail	9	14	39
External/Removable Media	2	0	0
Impersonation	0	NA	0
Improper Usage	89	115	40
Loss or Theft of Equipment	50	26	2
Web	11	7	4
Other	116	21	0
Multiple Attack Vectors	13	4	0
Total	291	187	87

CIO Self-Assessment

The Department of Education (Department) has continued its work to implement a comprehensive set of solutions to strengthen the overall cybersecurity of its networks, systems and data.

The Department has made significant improvements in the area of risk management. This effort included the implementation of the risk scorecard as a risk management tool that leverages the NIST Cybersecurity Framework to establish a quantitative methodology for identifying, analyzing and managing system-level cybersecurity risks across the framework's five core security functions. The Department utilizes the risk scorecards to perform regular framework-based risk assessments to identify security gaps and opportunities to enhance the Department's cybersecurity capabilities and better protect its network assets and data. Risk scorecards are reviewed biweekly by Department senior leadership.

In addition, the Department worked in close partnership and coordination with the DHS to complete formal Risk and Vulnerability Assessments and Security Assessment Reports for a number of the Department's HVAs. In addition to the DHS conducted reviews, the Department's CIO meets with each HVA system owner on a quarterly basis to thoroughly review system risks and mitigation plans.

Finally, through the IT Modernization effort, the Department hopes to reduce the IT footprint, thereby reducing cybersecurity risk by consolidating IT services and systems.

Independent Assessment

The objective of the independent assessment was to determine whether the Department's and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. The Office of Inspector General (OIG) assessed the effectiveness of security controls based on the extent to which the controls were implemented correctly, operated as intended, and producing the desired outcome with respect to meeting the security requirements for the information systems we review in their operational environment. The OIG found that the Department and FSA were not effective in any of the five security functions. They also identified findings in all eight metric domains, of which seven are repeat findings.

The Department demonstrated some improvement from fiscal year 2017 in several metric areas, most notably in contingency planning where the maturity level improved from Defined to Consistently Implemented. Although the Department and FSA made progress in strengthening their information security programs, we found areas needing improvement in all eight metric domains.

Specifically, the OIG found that the Department and FSA can strengthen their controls in areas such as its (1) remediation process for its Plan of Action and Milestones; (2) use of unsecure connections and appropriate application connection protocols; (3) reliance on unsupported operating systems, databases, and applications in its production environments; (4) protecting personally identifiable information; (5) consistent performance of system patching; (6) implementing the Identity, Credential, and Access Management strategy; (7) implementing a process to manage privileged accounts; (8) implementing two-factor authentication; (9) removing access of terminated users to the Department’s network; (10) fully implementing the Continuous Diagnostics and Mitigation program, and (11) ensuring data loss prevention tools work accordingly.

FY 2018 Annual Cybersecurity Performance Summary

Department of Energy

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	High Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	8	4	1
E-mail	99	64	79
External/Removable Media	4	0	0
Impersonation	7	NA	0
Improper Usage	80	102	172
Loss or Theft of Equipment	197	167	191
Web	151	75	42
Other	73	131	161
Multiple Attack Vectors	1	1	1
Total	620	544	647

CIO Self-Assessment

The Secretary has continued to stress cybersecurity as an agency priority and leadership plays an active role in shaping cybersecurity risk management and mitigation activities.

DOE faces many cyber threats including espionage from nation states, advanced persistent threats, and disruptive non-state actors. Successful attack by a cyber threat actor could result in damage, disruption, or unauthorized access to business/mission critical assets associated with the integrity and safety of personnel, nuclear weapons, energy infrastructure, and applied scientific R&D.

DOE is a federated and diverse enterprise, comprised of 97 entities across 27 states with 24 identified HVAs aligned to DOE mission essential functions. DOE is actively engaged with the DHS and OMB HVA team and HVAs are being integrated into the DOE FISMA compliance processes and ISCM.

Internal/external assessments identified below average management of hardware and software, configuration management, vulnerability and patch management, web application integrity, access controls, continuous monitoring, risk management, and performance monitoring as common shortfalls. Additionally, DOE OCIO identified and is addressing outdated cybersecurity policies and incident response planning and implementation.

In FY18 DOE directed the entire Department to participate in the DHS Continuous Diagnostics and Mitigation program, overwriting previous direction to only include DOE HQ components. As Phase I CDM tools are implemented across DOE, significant improvements in ISCM will be realized for the entire DOE enterprise, including its HVAs.

Additionally, DOE is reviewing/updating its cybersecurity policies. OCIO released a Cybersecurity Strategy and Implementation Plan for 2018-2020, began re-writing the DOE Cybersecurity Order and drafted a DOE Incident Response Plan. Lastly, OCIO is maturing its enterprise architecture office and IT modernization work-streams.

Independent Assessment

The information security program of the Department of Energy was evaluated as effective. The OIG conducted the annual evaluation of the Department of Energy's unclassified information security program and obtained results from the Department's Office of Enterprise Assessments concerning the Department's national security systems. We reviewed the Department's progress towards meeting the DHS/OMB FISMA metrics at five sites to assess the effectiveness of information security policies, procedures, and practices. Overall, the OIG determined that the Department was generally effective in implementing a cybersecurity program.

While improvements should continue to be made, we found that the Department had Consistently Implemented (Level 3) each the following functions: Identify; Protect; Detect; and, Recover. We found that the Department had achieved a Managed and Measurable maturity level for the Respond function. Because of the non-homogeneous nature of the Department's population, it is likely that the weaknesses discovered at certain sites reviewed may not be representative of the Department's enterprise as a whole and the overall results could change from year to year depending on which locations are tested by the OIG. The rating for each of the metrics includes the results of both unclassified and national security system environments.

FY 2018 Annual Cybersecurity Performance Summary

Department of Health and Human Services

Framework	CIO Rating	IG Rating
Identify	At Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	6	14	14
E-mail	693	1,120	885
External/Removable Media	9	5	16
Impersonation	7	NA	26
Improper Usage	1,445	2,575	3,588
Loss or Theft of Equipment	884	651	823
Web	1,458	907	1,263
Other	3,466	1,952	3,063
Multiple Attack Vectors	153	72	0
Total	8,121	7,296	9,678

CIO Self-Assessment

The Department of Health and Human Services (HHS) and its Operating Divisions are tasked with managing and protecting the country's critical information and public health care system. The management of these systems require HHS to protect High Value Assets (HVAs) from malicious actors who have a criminal interest in these systems. Increased network connectivity has expanded the government's capacity to store and process data however, this advent has led to federal agencies and their HVAs being exposed to more cyber risks-- including threats such as adversary and criminal interest, phishing, and network and software vulnerabilities. HHS has taken steps to mitigate these risks by developing collaborative efforts within HHS to manage its mission critical systems and HVAs that support our Mission Essential Functions (MEF).

Collaboration efforts also include working alongside DHS which provides operational assessment services and technical assistance to help manage cyber risk. HHS has also ensured that cybersecurity and privacy risks are captured and addressed within its Enterprise Risk Management framework. HHS has taken steps to familiarize itself with its HVA landscape by performing analysis based on DHS BOD 18-02 data elements to become aware of critical features such as system interdependencies, whether systems support MEFs, and whether functional exercises are performed in the event a system needs recovery.

HHS also performs reviews of contractual language for appropriate clauses relating to third party vendors and adherence to departmental policy. Additionally, HHS is working actively with a broad coalition of partners to enhance cybersecurity within the Department and across the Healthcare and Public Health Sector. HHS continues to work across the sector to raise awareness of the cybersecurity threats and tackle the shared challenges collaboratively. HHS is committed to the security and resiliency of the agency and the health care community.

Independent Assessment

Based on the results of our evaluation, we determined that HHS's information security program was 'Not Effective' since it was not at a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas. We did determine that HHS was "Consistently Implemented" in the Identify and Protect areas. FY18 FISMA annual audit reflects the assessment of 4 of the 12 HHS Operating Divisions and not the entire agency. HHS is a federated environment which brings challenges in attaining a "Managed and Measurable" maturity model for all Operating Divisions. Overall, HHS continues to implement changes to strengthen its enterprise-wide information security program.

HHS continues to be aware of the opportunities to strengthen its overall information security program to ensure that its policies and procedures at all Operating Divisions are consistently implemented in all areas of its security program. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS to include continuous monitoring of its networks and systems, documenting progress to address and implement strategies, and reporting its progress through DHS dashboards. Attaining a "Managed and Measurable" maturity level is dependent on the full implementation of CDM, which has its own challenges. HHS needs to ensure that there is effective contingency planning, identity and access management, configuration management, and incident response through the use of appropriate tools, processes, and controls at all Operating Divisions. HHS also needs to continue to build towards a working model where all the functional areas interact with each other in real-time and provide holistic and coordinated responses to security events. This will help to strengthen all aspects of its information security program in order for HHS to achieve its mission through an effective and coordinated information security program.

FY 2018 Annual Cybersecurity Performance Summary

Department of Homeland Security

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	1	2	0
E-mail	79	241	477
External/Removable Media	18	13	9
Impersonation	0	NA	0
Improper Usage	130	407	143
Loss or Theft of Equipment	5	16	14
Web	42	124	64
Other	818	1,245	420
Multiple Attack Vectors	19	57	0
Total	1,112	2,105	1,127

CIO Self-Assessment

In Fiscal Year 2018, DHS received a "managing risk" rating from the Risk Management Assessment. The agency has implemented action plans to improve the scores of the remaining cybersecurity framework functions rated 'at risk'.

In the Protect function, DHS continues to expand the visibility of enterprise-wide cybersecurity risks by standardizing toolsets used to manage mobile assets and configurations from the Continuous Diagnostics and Mitigation (CDM) program. Currently, DHS is highly dependent on components to manage cybersecurity threats and vulnerabilities. With the implementation of CDM, this challenge will be mitigated as there will be greater and more frequent visibility into threats and vulnerabilities facing the entire organization. DHS now relies on automated hardware asset inventories and unauthorized hardware alerts in some components through implemented CDM auto-discovery capabilities being reported in dashboards.

The Respond and Recover function was rated "at risk" because a critical vulnerability was not remediated within 30 days. The risk from this vulnerability is low and remediation will be completed through the replacement of the legacy system in FY19.

DHS actively monitors ATO status of FISMA systems and usage of improper operating systems in monthly cybersecurity reports and works with its components to manage risks and vulnerabilities that have direct impact on cybersecurity risk posture of the Department. Escalation processes are in place to address cybersecurity weaknesses of components on a recurring basis. DHS implementation of CDM is in progress and will provide a near real-time view of systems operating on DHS network but are outside an authorized to operate boundary.

The agency has updated its Information Security Performance Plan (ISPP) for FY2019, allowing agency executives more visibility on IT risks impact their mission space.

Lastly, DHS offers pay incentives to recruit and retain cybersecurity professionals. The Federal sector continues to face challenges in filling vacant cybersecurity positions due heavily to competing civilian entities that vie for industry skilled personnel. The implementation of pay incentives will enable the department to be competitive in the market to attract and retain highly qualified cybersecurity personnel.

Independent Assessment

The information security program of the Department of Homeland Security was evaluated as effective. DHS' progress in information security can be attributed to improvements in the areas of risk and configuration management. However, DHS components still do not effectively manage and secure their information systems – an ongoing problem since the Department's inception in 2003.

Specifically, components continue to operate systems without ATOs, use unsupported operating systems that may expose DHS data to unnecessary risks, ineffectively manage the POA&M process to mitigate identified security weaknesses, and do not apply security patches timely. The continuing deficiencies are contrary to the President's Cybersecurity Executive Order and clear indicators that departmental oversight of the enterprise-wide information security program needs to be strengthened.

Until DHS addresses its systemic information security weaknesses, it will remain unable to ensure that its information systems adequately protect the sensitive data they store and process. The OIG performed fieldwork at the DHS OCIO and at selected components. As part of our review, we interviewed key personnel, assessed DHS' current operational environment and compliance with FISMA requirements, and performed security testing to evaluate the effectiveness of controls implemented on selected systems.

FY 2018 Annual Cybersecurity Performance Summary

Department of Housing and Urban Development

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Consistently Implemented
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	1
E-mail	20	18	7
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	2	41	49
Loss or Theft of Equipment	2	5	4
Web	1	11	9
Other	56	94	25
Multiple Attack Vectors	5	4	1
Total	86	173	96

CIO Self-Assessment

In FY 2018, the Department of Housing and Development (HUD) continued the proactive implementation of the CSF as mandated by EO 13800, to manage the Department's cybersecurity risk. Additionally, the OCIO has established a Risk Officer to work with the Department's Risk Executive Officer to ensure that cybersecurity risks are visible and addressed at the Department level.

To further expand the OCIO's ability to proactively address cybersecurity risk, the Enterprise-wide Cybersecurity Independent Verification and Validation (IV&V) program was established. The Cybersecurity IV&V program takes a critical look at every facet of HUD's cybersecurity program to identify areas of concern pertaining to audit readiness, Cyber Defense, and the oversight to the implementation of the Cybersecurity Framework.

To proactively identify and mitigate risk associated with the Department's HVA and MES, the Department continues its participation in the following DHS US-CERT's National Cybersecurity Assessments and Technical Service's (NCATS) programs: HyperText Transfer Protocol Secure (HTTPS), Trustworthy Email Report, Cyber Hygiene, Einstein 3 Accelerated (E3A), and Continuous Diagnostic and Monitoring (CDM).

Independent Assessment

The information security program of the Department of Housing and Urban Development was evaluated as not effective. Key components of HUD's IS program remain ineffective or have inconsistent processes throughout the HUD program offices and among the many non-OCIO IT contractors. Significant limitations and challenges on the CIO's ability to establish an effective information security program continue to exist.

The lack of a mature Risk Management program contributes to HUD's inability to make informed, risk-based decisions and severely hinders their ability to efficiently and effectively modernize its legacy systems and establish information security program priorities. HUD also continues to experience vacancies in key IT leadership positions, such as the CISO position, which has been vacant for approximately 18 months. HUD, has been unable to obtain critical information security subject matter expertise, hindering the Department's ability to maintain continuity and mature its program knowledge.

HUD has made progress in improving portions of its governance, promotion of security awareness and the need for a strong information security culture. Also, HUD positioned itself to improve the maturity and associated effectiveness. The CIO position now reports directly to the Secretary which improves the chances of successfully prioritizing the modernization of HUD's IT infrastructure. HUD OCIO has begun focusing on the modernization of IT assets and was awarded $20 million through the OMB Technology Modernization Fund (TMF) program. HUD also increased the maturity of its incident response program, which was identified as a risk in the 2017 FISMA evaluation.

OIG recommends that HUD prioritize its information security program by continuously assessing and maturing the FISMA domains and require the program offices and contractors to consistently implement processes and procedures.

FY 2018 Annual Cybersecurity Performance Summary

Department of Justice

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	1	6	6
E-mail	119	339	610
External/Removable Media	3	1	0
Impersonation	0	NA	1
Improper Usage	685	513	175
Loss or Theft of Equipment	2,022	1,267	42
Web	144	61	82
Other	313	457	270
Multiple Attack Vectors	14	30	2
Total	3,301	2,674	1,188

CIO Self-Assessment

The Department of Justice (DOJ) has a strong cybersecurity risk management program, with enterprise-wide visibility and automated management of over 96% of the IT assets. Through this program, the Department tracks key performance indicators, such as secure configuration settings and critical vulnerabilities, which are measured and summarized into a risk score that reflects the overall security posture of DOJ. Over the last five years, DOJ has reduced the risk score by over 70%, demonstrating the Department's success at managing and reducing risk.

In FY18, DOJ made improvements in several key areas. DOJ deployed new identity management capabilities with an emphasis on identifying and managing privileged users. The Department modernized our legacy Trusted Internet Connection service to a cloud optimized service with full redundancy and the capacity to securely connect to all external networks. DOJ completed its HVA Overlay assessments, and tracked the progress of all HVA Plan of Actions and Milestones in our continuous monitoring tool, Cyber Security Assessment Management (CSAM). DOJ is committed to working with the Office of the Inspector General, the Office of Management and Budget, and the Department of Homeland Security to further strengthen and augment our security and privacy programs in the upcoming fiscal year.

Independent Assessment

The information security program of the Department of Justice was evaluated as not effective. During fiscal year 2018, the Department OIG reviewed the information security programs of 6 Department components and a sample of 15 systems within these components.

The Department should implement our recommendations specifically within the Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, and Contingency Planning metrics of to improve the effectiveness of the Department's information security program.

FY 2018 Annual Cybersecurity Performance Summary

Department of Labor

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	2
E-mail	60	23	35
External/Removable Media	0	2	0
Impersonation	1	NA	0
Improper Usage	4	53	81
Loss or Theft of Equipment	92	117	100
Web	7	6	16
Other	118	97	50
Multiple Attack Vectors	11	6	0
Total	293	305	284

CIO Self-Assessment

In FY18 the Department of Labor (DOL) enhanced its IT management and security capabilities by acquiring and implementing enterprise solutions that enable automation and near real-time vulnerability and IT asset awareness; connect security and IT resources; improve the speed and efficiency of security responses; and continue to enhance visibility into the security posture of the enterprise IT systems.

DOL continues its approach to strengthen the IT infrastructure with the implementation of an enterprise platform that provides for a significant reduction in infrastructure attack surface, and the ability to instantly bring back systems that have been attacked at near full production performance.

In FY 18, DOL completed implementation of additional Identity and Access Management (IAM) tools which affords the Department the capability of integrating DOL applications, leading to the centralization of Access Control functions and reduction of operational risk for managing accounts. DOL implemented Simplified Sign-On for nine applications in FY18, and expects to implement additional IAM capabilities in FY19.

Information Security Continuous Monitoring (ISCM) remains of particular importance in FY18 as DOL continues to leverage DHS monitoring capabilities while also becoming a more technological homogenous department. As in FY17, the Department focused more on capability effectiveness rather than on implementation as DOL sought to mature the ability to provide a more real-time and more expansive tactical approach to our ISCM.

Independent Assessment

In accordance with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, DOL has “Consistently Implemented” (maturity Level 3) its information security program and practices for the 5 Cybersecurity functions and 8 FISMA program areas. However, the program is rated overall as “Not Effective” since the majority of the 5 Cybersecurity functions were not assessed at Managed and Measurable (Level 4) or Optimized (Level 5).

FY 2018 Annual Cybersecurity Performance Summary

Department of State

Framework	CIO Rating	IG Rating
Identify	At Risk	Ad Hoc
Protect	Managing Risk	Defined
Detect	Managing Risk	Ad Hoc
Respond	At Risk	Consistently Implemented
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	1	8	36
E-mail	116	2,598	3,082
External/Removable Media	1	8	2
Impersonation	0	NA	0
Improper Usage	240	525	514
Loss or Theft of Equipment	2	27	22
Web	89	281	353
Other	543	877	541
Multiple Attack Vectors	11	81	10
Total	1,003	4,405	4,560

CIO Self-Assessment

Four of the five recommendations in the FY18 Cybersecurity Risk Management audit call for realignment of effort to the "Identify" area in risk and inventory management. To address these recommendations, the Department of State (DOS) funded and expanded the risk management program, implemented a revised cybersecurity risk management strategy, and integrated this strategy with enterprise-wide, risk management activities in accordance with OMB Circular A-123.

To directly target auditor findings, DOS enhanced inventory management capabilities through expanding resources allocated to agency-wide inventory and asset tracking. In addition, risk-based prioritization of systems was implemented to reduce the backlog of system assessment and authorizations. To improve security protections and system resilience, the DOS launched a new identity management system and accelerated modernization of legacy systems and remote access platforms.

On a daily basis, DOS is a growing target for threat actors worldwide, and incidents by attack vector increased in nearly every category. In FY18, DOS continued to mature and enhance global security monitoring and incident response programs to proactively detect, respond, and recover from these expanded threats. DOS increased the frequency of vulnerability scanning to identify potential security weaknesses and better detect suspicious network activity with an emphasis on High Value Assets.

For overseas posts, DOS enhanced daily reporting and customized assessments on cyber threat issues affecting DOS's critical, global infrastructure. Using cyber intelligence and threat data, DOS developed indicators and early warnings about potential cyber incidents and now performs expanded, in-depth assessments of network intrusion activity to better detect threats.

The remaining recommendation has been resolved and closed by the OIG.

Independent Assessment

The information security program of the Department of State was evaluated as not effective. Acting on behalf of the Office of Inspector General, an independent assessor conducted this audit to determine the effectiveness of the Department's information security program and practices in accordance with FISMA requirements in FY 2018. The independent assessor concludes that the Department does not have an effective organization-wide information security program for several reasons. OIG made five recommendations to improve Department's information security program.

FY 2018 Annual Cybersecurity Performance Summary

Department of State Office of Inspector General

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Optimized
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	3
Web	0	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	0	0	4

CIO Self-Assessment

The Department of State Office of Inspector General (OIG) faces cybersecurity risks that are common across the Federal Government. While OIG employs a defense-in-depth cybersecurity strategy to prevent and mitigate threats, residual risks from threats such as spear phishing, user access to malicious web sites, insider threats (unintentional and intentional), and zero-day threats persist.

The OIG took several actions in FY 2018 to mitigate cybersecurity risks, including the implementation of additional threat intelligence feeds, regular phishing exercises, enhanced training for all new-hires and contractors, implementation of the NIST Cybersecurity Framework, and third-party security penetration testing. In addition, an independent third-party assessed the OIG at maturity level 5 (Optimized) across all five Functions of the FY18 FISMA IG metrics, indicating 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.

- OIG subscribes to multiple threat intelligence feeds to identify and block emerging threats in real-time.
- OIG implemented an enterprise-wide phishing program to improve user resilience against top cybersecurity threats and provides real-time training to improve user education.
- OIG implemented an enhanced cybersecurity and privacy awareness training for all new-hires and contractors. This training amplifies user annual cybersecurity training requirements and emphasizes user data protection requirements and incident reporting responsibilities.
- OIG implemented the NIST Cybersecurity Framework by completing an analysis of current and desired states for maturity metrics across all Framework functions.
- OIG completed third-party penetration testing to review and validate OIGNet security architecture and defenses.

Independent Assessment

The information security program of the Department of State Office of Inspector General was evaluated as effective. As independent auditors, we conducted 2018 IG FISMA Metrics Assessment and determined that OIG regularly reviews, updates and shares its policies and procedures, consistently implements the security controls, manages and measures through effective metric reporting, and deploys automation, where necessary and safe, to support sustainable continuous monitoring and cybersecurity practice. There were no significant deficiencies found during the audit. OIG has witnessed significant but balanced growth in resources (people, processed and technology) to support OIG mission.

During interviews, demo, review of artifacts/evidence, we noted effective cybersecurity and integrated enterprise risk management practices, demonstrating optimization and continuous improvement in virtually all domain areas, including “Data Protection and Privacy”. OIG followed through 2017 IG FISMA Metrics recommendations to implement advanced technologies over these past 12 months that have added visibility and alerts for cyber, operations and helpdesk teams to collaborate and contain risks in an evolving threat landscape. 2018 IG FISMA Metrics audit reflected solid cybersecurity and risk management frame of mind in thought and action. We did identify areas of improvement through recommendations and recognized that highest metric level may not be accomplished for a particular metric, OIG has implemented defense-in-depth architecture to be effective and exceed OIG mission expectations.

FY 2018 Annual Cybersecurity Performance Summary

Department of the Interior

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Managed and Measurable
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Defined
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	2	0
E-mail	71	47	4
External/Removable Media	0	4	0
Impersonation	0	NA	0
Improper Usage	26	81	143
Loss or Theft of Equipment	22	14	18
Web	49	176	68
Other	133	175	172
Multiple Attack Vectors	9	12	2
Total	310	511	407

CIO Self-Assessment

The Department of the Interior (DOI) experienced no major incidents or privacy breaches, and there were no significant compromises during this reporting period. Additionally, the DOI OCIO closed 100% its FY2018 scheduled goal base.

Interior implemented 100% of DMARC blocking per BOD-18-01 for all enterprise email clients. In our implementation of DHS selected and mandated cyber-security tools under the CDM program, the DOI remains among the early adopters for these capabilities as they become available and viable.

Our confidence in the completeness of system inventories is reduced because the processes for identifying and registering systems relies upon subjective decisions and manual processes. To address this matter, we will be leveraging tools under the CDM program to discover and report systems more fully.

To ensure full visibility of progress toward mandated goals, we have implemented monthly cyber security briefings (with the Information Management and Technology Leadership Team (IMTLT) and Departmental leadership) that directly parallel the FISMA metrics.

The CIO position became vacant on September 16, 2018. The announcement for her successor closed on October 10, 2018. We anticipate the selection of a new CIO in the near future.

Independent Assessment

The information security program of the Department of the Interior was evaluated as not effective. A Performance Audit was conducted over the information security program and practices of the Department of the Interior (DOI) to determine the effectiveness of such programs and practice for the fiscal year ending September 30, 2018. The scope of the audit included the following Bureaus and Offices, Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), National Park Service (NPS), Office of the Inspector General (OIG), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), Office of the Special Trustee for American Indians (OST), and U.S. Geological Survey (USGS). DOI had 123 operational unclassified information systems and 11 information systems were randomly selected for the audit.

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, DOI established and maintained its information security program and practices in the five cybersecurity functions. However, the program was not fully effective as deficiencies were identified in each cybersecurity function area. Deficiencies were noted in the FISMA domain areas of risk management, configuration management, data protection and privacy, information security continuous monitoring, incident response, and contingency planning metric domains.

FY 2018 Annual Cybersecurity Performance Summary

Department of the Treasury

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	1
E-mail	10	10	5
External/Removable Media	10	0	0
Impersonation	0	NA	1
Improper Usage	15	95	114
Loss or Theft of Equipment	315	95	16
Web	22	8	5
Other	226	248	43
Multiple Attack Vectors	4	2	0
Total	602	459	185

CIO Self-Assessment

The mission of the Department of the Treasury is to maintain a strong economy and create economic and job opportunities by promoting conditions that enable economic growth and stability at home and abroad; strengthen national security by combating threats and protecting the integrity of the financial system; and manage the U.S. government's finances and resources effectively. To execute its mission, Treasury must store, process, transmit, and share large volumes of highly sensitive financial and personal information affecting the transaction of trillions of dollars. Mission execution faces evolving cybersecurity risks inherent in the need to interact with private and other public sector organizations, limitations of authentication technologies, reliance on externally managed critical infrastructure, and a current lack of centralized visibility of agency information technology assets and networks in need of modernization.

The likelihood of risk realization is magnified by the continuous evolution in the volume, sophistication, and frequency of cyber threats targeting the U.S. government. The Department's senior leadership is consistently engaged in the development of plans to address these risks, but appropriate mitigation will require additional investment of resources over the next several years to enhance and expand defensive capabilities and to recruit, maintain, and retain an adequately trained workforce. In FY 2018, the Department began leveraging investments from the Cybersecurity Enhancement Account to introduce new defensive capabilities. These investments will continue throughout FY 2019 as the capabilities begin to come online.

Independent Assessment

The information security program of the Department of the Treasury was evaluated as not effective.

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for its unclassified systems for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program and practices were not fully effective as reflected in the deficiencies that we identified in Risk Management, Configuration Management, Identity and Access Management, and Contingency Planning. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The IRS's Cybersecurity Program was generally in alignment with FISMA requirements, but it was not fully effective due to program attributes not yet implemented.

Consistent with applicable FISMA requirements, OMB and CNSS policy and guidance, and NIST standards and guidelines, Treasury has established and maintained its information security program and practices for its Collateral NSS for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program was not fully effective as reflected by the deficiencies that we identified in the Risk Management, Identity and Access Management, and Incident Response, program areas. In addition, we did not assess any of the FISMA Metric Domains as Managed and Measurable (Level 4). The FY 2018 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable (Level 4).

FY 2018 Annual Cybersecurity Performance Summary

Department of Transportation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	1
E-mail	8	49	27
External/Removable Media	0	3	0
Impersonation	0	NA	2
Improper Usage	7	111	172
Loss or Theft of Equipment	9	71	93
Web	5	130	174
Other	160	297	324
Multiple Attack Vectors	3	11	10
Total	192	673	803

CIO Self-Assessment

The Department of Transportation (DOT) implemented changes in its oversight, review, and validation of data and responses for the annual FISMA reporting cycle and audit, enhancing agency-level controls to improve the quality of information reported to OMB and to the OIG. The resulting process changes have produced a reduction in erroneous submissions, ensured timely escalation of actions for incomplete or missing responses, and improved the overall analysis and representation of the agency's cybersecurity program and posture. DOT also continued implementation of its Network Assessment Risk Mitigation (NARM) initiative to modernize DOT networks, with recent improvements focused on network visibility, orchestration, and automation.

In support of cybersecurity for the Transportation Sector, the Department has acted to clarify roles and responsibilities for transportation sector cybersecurity within the Office of the Secretary. The Department has gained additional visibility into cybersecurity-related activities within individual DOT component operating administrations (OAs) and has been asserting coordination across the Department, and from the Department to DHS, OMB, and the National Security Staff. The result has been to elevate the visibility of cybersecurity at the Department level, and to support additional collaboration to include the coordination of agency transportation research efforts with a cybersecurity focus.

The Federal Aviation Administration (FAA) has expanded the membership and oversight processes of the FAA Cybersecurity Steering Committee, adding the FAA Airports organization as a permanent member, and creating a High Value Risks (HVR) program to capture, assess, manage, and mitigate critical and high risks within FAA systems and networks. The Committee, which includes the DOT CISO as a member, has also led collaboration with DHS and the Department of Defense (DoD) to update the charter for the Aviation Cybersecurity Initiative (ACI). The initiative seeks to improve the identification and mitigation of cybersecurity risks and threats within the aviation subsector.

Independent Assessment

The information security program of the Department of Transportation was evaluated as not effective. DOT has made progress in its information security program. The rigorous, scaled nature of the metrics is not designed to capture the improvements and movement towards higher levels of maturity; hence, progress is not apparent in the scoring. On the other hand, there are areas of stagnation which are weighing down on DOT's level of maturity.

FY 2018 Annual Cybersecurity Performance Summary

Department of Veterans Affairs

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	3
E-mail	731	614	358
External/Removable Media	49	19	4
Impersonation	17	NA	3
Improper Usage	53	107	75
Loss or Theft of Equipment	419	394	362
Web	1,015	723	239
Other	455	773	732
Multiple Attack Vectors	69	30	0
Total	2,808	2,661	1,776

CIO Self-Assessment

VA operates a robust enterprise-wide Risk Management Framework (RMF) program that is fully aligned with NIST guidelines to include NIST SP 800-37, 800-53, 800-53A, 800-39, 800-30, and 800-60 as well as FIPS 199 and 200. Currently, VA information systems operate under valid ATO and any residual risk is being monitored and managed via system-specific Plans of Actions and Milestones.

VA identified the Department's High Value Assets (HVAs) and Mission Essential Functions (MEFs) in accordance with the 2017 OMB M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure". Since then, VA continues to be proactive in the management of cybersecurity risk to the Department's HVAs and MEFs, in alignment with the 2018 DHS BOD 18-02, "Securing High Value Assets". Additionally, VA engaged DHS in October 2018 to perform RVAs against VA HVAs and MEFs. DHS has selected three HVAs and has begun assessments on these, while VA is prepared to support and resolve findings as needed.

VA will address the DHS RVA findings through ongoing activities within VA's Enterprise Cybersecurity Strategy Program (ECSP). These activities include further segmenting VA's network and supplementing VA data loss prevention tools to strengthen the security of VA's infrastructure and modernize information technology. As VA's ECSP is refreshed, these activities will be continually assessed and enhanced in a prioritized manner, based on VA's risk management process, to continue the protection of HVAs and MEFs.

Independent Assessment

The information security program of the Department of Veterans Affairs was evaluated as not effective. The OIG assessed VA's information security program through inquiries, observations, and tests of selected controls supporting major applications and general support systems at 24 VA facilities.

VA has made progress developing policies and procedures but still faces challenges implementing components of its agency-wide information security continuous monitoring and risk management program to meet FISMA requirements. While some improvements were noted, this audit identified continuing significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems. Weaknesses in access and configuration management controls resulted from VA not fully implementing security standards on all servers, databases, and network devices. VA also has not effectively implemented procedures to identify and remediate system security vulnerabilities on network devices, databases, and server platforms VA-wide.

FY 2018 Annual Cybersecurity Performance Summary

Election Assistance Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Consistently Implemented
Detect	At Risk	Defined
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

EAC filled the position of CIO at the beginning of this fiscal 2019 year. She is charged with assisting the Election Assistance Commission (EAC) with FISMA and hardening cybersecurity and operations to include government wide Binding Operational Directives.

The EAC has instituted many policies and procedures that correspond with the FISMA Enterprise Risk Strategy (ERS) requirement. The EAC currently has approved and published a full Strategic Plan, 2018- 2022.

In addition, the EAC has implemented a Security Assessment Report (SAR), and several other technical procedures that categorize and mitigate risk. Many of the required ERS initiatives are developed.

Moreover, in an effort to enhance enterprise risk, the EAC is working with the OPM to perform an assessment. The OPM assessment involves a detailed examination of the agency's staffing needs to accomplish HAVA's requirements, as directed by the Commissioners in the February 24, 2015, Organizational Management Policy Statement. The OPM study will greatly assist the EAC in identifying how best to: strategically align staff roles and responsibilities; manage risk with succession planning; and implement other agency specific efficiencies. The EAC is also working on implementing organizational and system-level business impact assessment as part of the risk identification process. However, the EAC recognizes a consolidated and final ERS is required to achieve FISMA compliance.

Independent Assessment

The information security program of the Election Assistance Commission was evaluated as effective. EAC generally complied with FISMA requirements by implementing selected security controls for tested systems. Although EAC generally had policies for its information security program, its implementation of those policies for selected controls was not fully effective.

FY 2018 Annual Cybersecurity Performance Summary

Environmental Protection Agency

Framework	CIO Rating	IG Rating
Identify	At Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	0
E-mail	22	27	5
External/Removable Media	3	2	0
Impersonation	7	NA	1
Improper Usage	9	34	41
Loss or Theft of Equipment	11	31	63
Web	153	126	14
Other	16	121	41
Multiple Attack Vectors	0	1	0
Total	221	343	165

CIO Self-Assessment

System level risks, including those to HVAs supporting MEFs, have been determined to be at acceptable levels, though there are many unknown risks due to EPA's limited cybersecurity capabilities, including the ability to sufficiently identify and mitigate weaknesses. Major risk areas include: insufficient resources; detecting and alerting on unauthorized hardware and software; vulnerability management; identity and access management; insider threats; remote users; malware protection; exfiltration defenses; incident response; inadequate network capacity and architecture to support important security capabilities; legacy and emerging technologies; acquisitions processes, contracts, and contractor oversight; and sub-optimal staffing levels, skills, and organization. Furthermore, increased usage of mobile devices to meet mission needs could create additional risks.

EPA currently has significant gaps in cybersecurity capabilities, human resources, and supporting infrastructure. The Agency also has limited ability to gather quantitative data and relies on qualitative measures, leaving significant blind spots. Additionally, low funding levels limit the scope of the Agency's Security Operations Center and Incident Response Team. While the CDM program is expected to help improve EPA's capabilities by providing continuous monitoring tools and dashboards, additional resources are required to provide the infrastructure, support operations, and maintenance of the tools and to develop and implement processes that can turn the resulting data into meaningful actions.

The Risk Executive Group (REG) and the CIO are integral components of EPA's cybersecurity risk management strategy. The REG assesses risk and provides recommendations to the CIO, who provides risk mitigation guidance to program office and region Authorizing Officials and reviews and approves the cybersecurity risk management strategy. Senior Executive Authorization Officials make system-level authorization decisions. The CISO monitors information security compliance, assesses control statuses, threats, and risks and makes recommendations to the Risk Executive/CIO. Furthermore, the CISO disseminates cybersecurity status reports monthly to the Senior Executive Authorization Officials to provide objective information indicative of risk posture and enable better informed risk decisions. The EPA's Acting Deputy Administrator, who has been designated as the Senior Accountable Official for Risk Management, has instituted monthly meetings to review cybersecurity status and progress.

Independent Assessment

The U.S. Environmental Protection Agency (EPA) achieved an overall assessment of Maturity Level 3, which denotes that the agency consistently implements its policies, procedures and strategies within its information security program. However, the EPA can further improve its processes in the following domains to strengthen its information security posture:

- Risk Management—Implement standard data elements for hardware assets connected to the network and for software and associated licenses used within the agency's environment.
- Security Training—Implement a process for reporting on contractors' completion of role-based training.
- Incident Response—Implement certain technologies to support the incident response program.
- Contingency Planning—Implement a process to ensure that the results of business impact analyses are used to guide contingency planning efforts.

FY 2018 Annual Cybersecurity Performance Summary

Equal Employment Opportunity Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Consistently Implemented
Detect	At Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	3	1	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	1
Web	2	0	0
Other	14	3	1
Multiple Attack Vectors	1	0	0
Total	20	4	3

CIO Self-Assessment

In FY 2018, the EEOC continued to modernize its technology infrastructure and mitigate its major risks, including: (1) Following the recent implementation of Active Directory, EEOC implemented PIV device-based access for all privileged users. Further deployment of PIV authentication is pending the removal of Novell E-Directory dependencies from client devices, which will be completed in FY 2019; (2) Actively addressed vulnerabilities for compliance with BOD 18-01, including enabling HSTS, mitigating weak ciphers, and implementing "DMARC p=reject" settings. EEOC continues to work with third-party vendors to address the remaining items needed to achieve full BOD 18-01 compliance; (3) Engaged with DHS to fully implement E3A. The Agency previously completed E3A traffic aggregation and DNS sink-holding and initiated E3A email filtering in late FY 2018, with expected completion during the first quarter of FY 2019; and (4) EEOC procured and is in the process of deploying new CISCO switches, firewalls and the Identity Services Engine (ISE) platform to improve network access control and intrusion protection and detection. The Agency also acquired Office 365 Advanced Threat Protection, which includes sandbox/detonation functionality, and will be enabling it for all users in Q1 FY 2019. It presently is in use for all privileged users.

In compliance with BOD 18-02, the EEOC's Integrated Mission System (IMS) was designated as a HVA, due to its support of mission-essential functions related to charge, case, and complaint processing. Documents containing sensitive PII within the IMS content management repository are inventoried and encrypted at rest, strengthening privacy protections. No other sensitive PII is maintained within the IMS. The EEOC is in the process of conducting a comprehensive compliance review of IMS security control configurations against new HVA requirements.

Independent Assessment

The information security program of the Equal Employment Opportunity Commission was evaluated as effective. The EEOC continues to make positive strides in addressing information security weaknesses, and the independent contractor found that EEOC generally had sound information security controls for its information security program. The EEOC information security program has an overall maturity level of "Managed and Measurable," however, EEOC needs to continue to improve in its ability to Protect (Data Protection/Privacy and Security Training) and Recover (Contingency Planning) its information systems.

FY 2018 Annual Cybersecurity Performance Summary

Export-Import Bank of the United States

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	1	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	1	0
Other	3	6	0
Multiple Attack Vectors	0	1	0
Total	4	10	0

CIO Self-Assessment

EXIM has taken numerous comprehensive steps to mitigate cybersecurity risks to the agency, and the improvement in scores from FY17 to FY18 are indicative of that effort. In FY18 at the information system level, EXIM continued working to implement an improved and robust Security Assessment and Authorization (SA&A) process for security control assessment of both internal and external EXIM systems. EXIM's cybersecurity team performed robust security control assessments and attained ATOs for vital EXIM systems, including FMS-NG, EOL, and the Infrastructure GSS. POA&Ms are documented and consistently reviewed to ensure information security risks at the system level are properly remediated in a timely fashion. At the agency level, EXIM provided comprehensive Security Awareness Training to 100% of EXIM employees and contractors, implemented a compliant enterprise Incident Response Plan, provided specialized Incident Response training, performed an executive-level Incident Response tabletop exercise, and continued to regularly review and update agency and program level security policies and procedures. EXIM also improved its vulnerability management and internal auditing processes, and updated and implemented an improved Information Security Continuous Monitoring (ISCM) program, among other activities. EXIM works with FISMA and FISCAM auditors to determine agency and program level weaknesses and develops action plans to remediate any findings. EXIM determined that the agency contains no High Value Assets (HVAs) in FY18.

Independent Assessment

The information security program of the Export-Import Bank of the United States was evaluated as not effective. Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, EXIM Bank has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA program areas. However, the program was not fully effective as reflected deficiencies that we identified in risk management, information continuous monitoring, incident response, and contingency planning metric domains.

FY 2018 Annual Cybersecurity Performance Summary

Farm Credit Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Managed and Measurable
Detect	At Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Managed and Measurable
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	18	3	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	0	1
Loss or Theft of Equipment	10	10	5
Web	1	0	0
Other	32	13	2
Multiple Attack Vectors	1	0	0
Total	63	26	8

CIO Self-Assessment

The Farm Credit Administration (FCA) is currently tracking 81 risks through its cybersecurity Risk Management Program. These risks are identified from several sources, such as on-demand risk assessments, open-source intelligence, assessment and authorization, penetration tests, and after-action incident reviews. The risks of highest significance to the organization center on FCA's safety-and-soundness, mission-essential function and the ability for its examiners to access and transfer relevant examination-related information to the FCA network for further evaluation. FCA is also tracking risks aligned with the NIST Cybersecurity Framework. The FCA risk register is reviewed by the CIO weekly. During these reviews, changes in risk factors are discussed.

The CIO discusses high-priority concerns with Senior Staff Members and FCA Board Members, as appropriate. As a result of our Risk Management Program, FCA has initiated risk mitigation in several areas, such as defending against ransomware by monitoring for and stopping excessive encryption. FCA is also mitigating the potential for unauthorized devices by initiating a network access control program. To ensure the security of examination data, FCA conducts intrusion prevention, encrypts sensitive database columns, and ensures TLS-encrypted connections with of our institutions. FCA also conducts mobile device management, including policy enforcement and remote wipe of lost devices.

Independent Assessment

The information security program of the Farm Credit Administration was evaluated as effective. The Farm Credit Administration (FCA or Agency) has an information security program that continues to mature. The OIG identified five actions the Office of Information Technology agreed to that will strengthen and improve the Agency's information security and privacy program in the domains of Identity and Access Management and Data Protection and Privacy.

FY 2018 Annual Cybersecurity Performance Summary

Federal Communications Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Consistently Implemented
Protect	At Risk	Managed and Measurable
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover	Managing Risk	Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	8
E-mail	3	3	5
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	3	2
Loss or Theft of Equipment	34	29	11
Web	2	5	5
Other	33	77	16
Multiple Attack Vectors	2	0	0
Total	74	117	47

CIO Self-Assessment

The FCC is exposed to similar cyber risks as other federal agencies from insider threats, external penetration risks, and exposure through internal control deficiencies both within the business processes and IT. The Commission has undertaken and continues to undertake extensive efforts to mitigate the risks through a combination of real-time assessments and compliance measures. These mitigation efforts include the implementation of internal controls across the IT architecture and landscape, leveraging the NIST 800-53 control set. Critical Systems include High Value Assets and Mission Essential Functions (MEF) such as Genesis, DIRS and the overall IT infrastructure. The FCC has executed full system-wide and defense-in-depth controls testing of these critical and high value asset systems to include annual Continuity of Operations and Disaster Recovery assessments. The Commission has also implemented additional security measures and network protections such as the implementation of security information and event management (SIEM), user authentication and privileged user ID remediation efforts, configuration baseline enforcement automated tools, asset management solution, network access controls, and enhanced firewalls. In addition, cloud security mechanisms such as Zscalar and Proofpoint was integrated into the security architecture.

Independent Assessment

The information security program of the Federal Communications Commission was evaluated as not effective. The FY 2018 FISMA evaluation included the Federal Communication Commission's (FCC) network (i.e., FCCNet), the FCC's core financial management system (Genesis), the Universal Service Administrative Company's (USAC) core financial management system (Great Plains), and a USAC support system (E-Rate Productivity Center [EPC]).

While the FCC made improvements to processes within its overall Information Security Program since the FY 2017 FISMA evaluation in the areas of risk management (i.e., system inventory), ISCM (i.e., metrics), and contingency planning (i.e., information system contingency plans), an independent auditor and the FCC OIG determined that the FCC's overall program was ineffective in FY 2018.

The independent auditor noted control weaknesses in each domain area within the five functions, with the exceptions of Data Protection and Privacy and Security Training. Going forward, we recommend that the FCC implement its documented security policies and procedures and establish ongoing monitoring over all five NIST Cybersecurity Functions to achieve an effective maturity Level 4, Managed and Measurable, for its Information Security Program.

FY 2018 Annual Cybersecurity Performance Summary

Federal Deposit Insurance Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	8	14	1
External/Removable Media	0	0	0
Impersonation	1	NA	1
Improper Usage	139	144	101
Loss or Theft of Equipment	108	31	0
Web	13	6	4
Other	22	33	8
Multiple Attack Vectors	0	0	0
Total	291	228	115

CIO Self-Assessment

Given the FDIC's mission as a financial regulator, cybersecurity risks to the FDIC are similar to those faced by other federal organizations and the financial industry at large. The risks to the FDIC span the cybersecurity spectrum to include: sophisticated and financially motivated threat actors, a complex mix of commercial and legacy assets, enterprise security architecture, and governance. The FDIC continues to prioritize and enhance its cybersecurity program to mitigate risks and emerging threats. Actions taken in FY 2018 include improvements to asset management, continued development and implementation of secure baseline configurations, establishing a new backup data center, enhancing breach and incident response practices, and a significant reorganization of the FDIC's cybersecurity workforce through the creation of the Office of the Chief Information Security Officer.

Recent assessments of FDIC cybersecurity controls identified the following areas warranting additional focus and resources:

- Configuration baselines and patch management,
- Enterprise Security Architecture,
- Common controls implementation,
- ERM,
- IT Asset Inventory Management,
- Modernization of Continuous Monitoring to include outsourced service delivery models such as cloud services, and
- Continue enhancements to Contingency Readiness.

Independent Assessment

The information security program of the Federal Deposit Insurance Corporation was evaluated as not effective. The OIG's audit covered key components of FDIC's information security program and selected security controls pertaining to three general support systems and one outsourced service provider. The FDIC established a number of information security program controls and practices that complied or were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines.

The FDIC also took or was working to take steps to strengthen its information security program controls following the FISMA audit conducted in 2017. For example, the FDIC established an agency-wide Incident Response Plan and updated its Breach Response Plan to address Federal policy requirements and guidelines; issued an Information Security and Privacy Strategic Plan that aligns with its IT Strategic Plan; and developed controls to help ensure the replacement or upgrade of software when vendors discontinue support.

However, weaknesses existed that limited the effectiveness of FDIC's information security program and practices and placed the confidentiality, integrity, and availability of its systems and data at risk. Weaknesses were identified in such areas as information security risk management, enterprise security architecture, security control assessments, patch management, and backup and recovery. The audit resulted in four recommendations to improve the effectiveness of FDIC's information security program and practices. The FDIC was also working to implement an additional nine outstanding recommendations from prior FISMA assessments.

FY 2018 Annual Cybersecurity Performance Summary

Federal Energy Regulatory Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	At Risk	Optimized
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	1
Other	5	5	0
Multiple Attack Vectors	0	0	0
Total	5	5	1

CIO Self-Assessment

In FY 2018, we continued to make significant investment in maintaining, evolving, and maturing our risk-based, cost effective cybersecurity program. Some highlights include: (1) Implemented a robust Security Information and Event Management (SIEM) tool to complement current log management technologies and improve situational awareness, (2) Deployed advanced malware protection to all critical production servers, utilizing global threat intelligence to strengthen agency defenses and to protect the organization before, during, and after an attack, (3) Fully integrated privacy into the agency Continuous Monitoring process, more accurately representing the overall agency security posture, and (4) Established trend analysis reporting for system risk on a monthly basis to assist in risk based decisions both at system and enterprise levels.

FERC continues to make progress toward meeting FY 2018 government-wide targets in the Cybersecurity Cross-Agency Priority Goal metrics. Our efforts in improving cybersecurity have continued to enhance the Commission's cybersecurity posture and support our compliance with FISMA, as is indicated by this year's report.

Independent Assessment

The information security program of the Federal Energy Regulatory Commission was evaluated as effective. The OIG conducted the annual evaluation of the Commission's unclassified information security program to assess the effectiveness of unclassified information security policies, procedures, and practices within five information security functions.

FY 2018 Annual Cybersecurity Performance Summary

Federal Housing Finance Agency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Optimized
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	0	0
Loss or Theft of Equipment	6	9	26
Web	1	0	0
Other	3	15	0
Multiple Attack Vectors	0	0	0
Total	11	24	26

CIO Self-Assessment

FHFA continues to make progress toward meeting Cybersecurity CAP Goal metrics. By the end of FY2018, FHFA had met all CAP Goal metrics with the exception of the following:

Software Asset Management: FHFA's Windows devices are configured with security tools with the capability to detect, alert and block unauthorized software. This is not applicable to the Mac OSX or UNIX environment. FHFA considers this a low risk given the low presence of malware on Mac OSX and UNIX operating systems.

Automated Access Management: FHFA does not currently employ a dynamic access management solution. This is an emerging security concept that FHFA will evaluate in FY19.

During FY2018, FHFA reported a total of 26 incidents to the United States Computer Emergency Readiness Team. These incidents consisted primarily of lost or stolen agency-issued mobile devices, none of which constituted a major incident.

Based on security and privacy program self-assessments and the OIG's independent review, I have determined with reasonable assurance that as of September 30, 2018, FHFA's information security and privacy policies, procedures, and practices are adequate and effective.

Independent Assessment

The information security program of the Federal Housing Finance Agency was evaluated as effective. An independent public accounting firm (IPA) under contract and supervision of the Federal Housing Finance Agency (FHFA) Office of Inspector General completed a performance audit to evaluate the effectiveness of FHFA's Information Security Program and practices and respond to the DHS FY 2018 IG FISMA Reporting Metrics, dated May 24, 2018. The IPA's methodology included testing the effectiveness of selected security controls implemented in a subset of systems in accordance with the NIST SP 800-53, Rev. 4. The IPA determined that FHFA's Information Security Program and practices were operating effectively, in compliance with FISMA, OMB's guidance, and sampled security controls selected from NIST SP 800-53.

FY 2018 Annual Cybersecurity Performance Summary

Federal Labor Relations Authority

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Managed and Measurable
Detect	At Risk	Managed and Measurable
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	1	0
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	1	1	0

CIO Self-Assessment

The FLRA continued to improve its overall security posture in several ways this year. We continued to move to our document management system which helped us increase our security by encrypting data both in transit and at rest. The FLRA also migrated its entire staff to Office 365 to utilize Microsoft's high availability for our email system. We continued to close findings on our Plan of Action and Milestones as well. The FLRA also engaged DHS and signed a Memorandum of Agreement for DHS's CDM solution and are currently on the waitlist to get the utilities up and running. In fiscal year 2018, the FLRA determined that it had no High Value assets.

Independent Assessment

The information security program of the Federal Labor Relations Authority was evaluated as effective. During our FY 2018 evaluation, the OIG noted that FLRA has taken steps to improve the information security program. The OIG also noted that FLRA does take information security weaknesses seriously. FLRA took action to remediate several weaknesses within specific control areas.

This year's FISMA testing included a follow up of all prior year recommendations. There were several new findings as follows:

- Timely deployment of patches;
- Rules of behavior lacking the latest guidance in accordance with National Institute of Standards and Technology (NIST);
- Lack of disabling users after 180 days of inactivity; and
- Lack of audit log reviews.

FY 2018 Annual Cybersecurity Performance Summary

Federal Maritime Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	2	0
Loss or Theft of Equipment	0	0	0
Web	3	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	3	3	0

CIO Self-Assessment

The FMC has taken numerous steps to combat the ever-present cybersecurity risk faced by most federal agencies such as viruses, malware, intrusion, compromised credentials, etc.

The FMC has moved to CenturyLink, a Managed Trusted Internet Protocol Services (MTIPS) certified internet service provider, in order to comply with the Trusted Internet Connection initiative.

The FMC has moved all email services to Microsoft 365. Microsoft 365 provides built-in malware and spam filtering capabilities that help protect inbound and outbound messages from malicious software and help protect our network from spam and other malicious files transferred through email.

The FMC is also compliant with DHS BOD 18-01 Trustworthy Email, Cyber Hygiene, and HTTPS/ HSTS Assessment created by the NCATS team inside the DHS NCCIC. FMC is currently in the process of implementing the Continuous Diagnostic and Mitigation program consistent with guidance from the OMB and NIST. The FMC also employs the Varonis DatAdvantage system. The Varonis DatAdvantage system continuously monitors the FMC network looking for the tell-tale signs of virus/ malware signature activity such as rights escalation, abnormal file access, and excessive data transfer, or excessive data encryption.

The FMC also employs Symantec Endpoint protection, and CylanceProtect 360. These are desktop virus scanning applications that are the best in the industry that are continuously running and monitoring every system on the network for the presence of viruses, malware, and other malicious files and malicious file activity.

Independent Assessment

The information security program of the Federal Maritime Commission was evaluated as effective. The overall IG assessment rating is "effective" for the Federal Maritime Commission (FMC). The scope of our testing focused on the FMC GSS and Major Applications. We conducted our testing through inquiry of FMC personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. More specifically, our testing covered a sample of controls as listed in NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4. Our testing was for the period October 1, 2017 through September 30, 2018 (fiscal year 2018). In the IG's fiscal year 2018 FISMA evaluation, the OIG identified four weaknesses, and concluded the FMC had effectively implemented one of the two prior year recommendations.

FY 2018 Annual Cybersecurity Performance Summary

Federal Mediation and Conciliation Service

Framework	CIO Rating	IG Rating
Identify	High Risk	Ad Hoc
Protect	At Risk	Managed and Measurable
Detect	At Risk	Ad Hoc
Respond	At Risk	Defined
Recover		Managed and Measurable
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

Federal Mediation and Conciliation Service has followed its cybersecurity framework action plan and has secured the services of several contractors who have performed cybersecurity assessments. The results of these assessments included an implementation plan to remediate identified risks and provide a mechanism for continued evaluation. One of the primary actions identified is the plan to implement a Managed Security Services Provider (MSSP) for continuous monitoring by the end of FY 2019. This will allow the Agency to respond in a comprehensive manner to any incidents identified by the MSSP. The Agency has identified and submitted High Value Assets per BOD 18-02 and integrated them into its cybersecurity framework. By performing these actions, the agency believes they have made significant progress towards achieving “Managed and Measurable” maturity.

Independent Assessment

The information security program of the Federal Mediation and Conciliation Service was evaluated as effective.

FY 2018 Annual Cybersecurity Performance Summary

Federal Mine Safety and Health Review Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	2	0
Multiple Attack Vectors	0	0	0
Total	0	2	0

CIO Self-Assessment

The Federal Mine Safety and Health Review Commission worked on BOD 18-01 compliance by implementing HSTS, enforcing HTTPS, and removing 3DES low encryption from the organization's domains.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Federal Mine Safety and Health Review Commission was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Federal Mine Safety and Health Review Commission will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Federal Retirement Thrift Investment Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Defined
Detect	At Risk	Ad Hoc
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	15	12
Loss or Theft of Equipment	2	13	18
Web	0	1	0
Other	24	75	2
Multiple Attack Vectors	0	0	0
Total	27	104	32

CIO Self-Assessment

In FY 2018, the Federal Retirement Thrift Investment Board (FRTIB, or "the agency") has made good progress on the implementation of the government-wide Cross Agency Priority (CAP) goals. Of the ten CAP Goals for FY 2018, the agency has achieved all but two, specifically

- Hardware Asset Management – the Agency encountered delays in its implementation of Network Access Control but is on track to complete this project in Q1 FY 2019
- Software Asset Management – the Agency will implement this capability through DHS' Continuous Diagnostics and Mitigation program in FY 2019.

Maturity in FISMA compliance and achievement of CAP goals will always remain a top priority for the agency, and focused efforts to the above will continue in FY 2019 (and beyond), with the goal of improving the Agency's maturity across all FISMA domains.

Independent Assessment

The information security program of the Federal Retirement Thrift Investment Board was evaluated as not effective. Although FRTIB made progress to its information security program during FY 2018, the independent assessors found that FRTIB did not fully develop and implement an effective, organization-wide program to identify, protect, detect, respond, and recover from information security weaknesses using a risk-based approach. In addition, FRTIB did not sufficiently implement governance structures to ensure appropriate oversight and monitoring over information security.

FRTIB undertook multiple projects to improve its information security posture during FY 2018. In particular, under Configuration Management, FRTIB developed an entity-wide configuration management plan to redefine the roles and responsibilities of Federal employees and third party contractors supporting its configuration management processes.

In addition, under Identify and Access Management, FRTIB completed Phase One of its ICAM Service and Capability Roadmap which resulted in the development of detailed requirements for FRTIB's ICAM practices and the definition of top tier roles and responsibilities. The maturity levels for these two domains increased from Level 1 (Ad-Hoc) to Level 2 (Defined). For FY 2018, the FISMA reporting metrics were updated to include a new FISMA domain, Data Protection and Privacy, and based on the audit procedures performed, the independent assessors concluded that the maturity level for this domain is Level 2 (Defined).

FY 2018 Annual Cybersecurity Performance Summary

Federal Trade Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Defined
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	1
E-mail	25	6	3
External/Removable Media	0	0	0
Impersonation	2	NA	0
Improper Usage	9	8	18
Loss or Theft of Equipment	1	0	0
Web	1	1	0
Other	32	6	1
Multiple Attack Vectors	3	2	0
Total	73	23	23

CIO Self-Assessment

While the Federal Trade Commission (FTC) has begun to manage the risk to Mission Essential Functions (MEF) by leveraging cloud service providers, the organization still relies on legacy IT and contracts for its on-premise data centers. The CIO Ratings highlight the impact of accepted risks with remaining legacy IT that limits FTC's ability to implement technical capabilities. FTC issued contract actions in FY2018 to improve its capabilities by migrating additional services to cloud offerings.

The Agency exercises discretion over its authorization process through changes in policy to cost-effectively manage FISMA compliance while undergoing IT modernization. For example, FTC accepts the compliance risk that internet traffic will not traverse MTIPS but will traverse a commercial policy enforcement architecture that accommodates high utilization of authorized cloud services. The agency will continue to pursue IT capabilities with strong authentication, inspection, and encryption at-rest and in-motion to minimize adverse impacts from network latency or bandwidth requirements.

Independent Assessment

The OIG assessed the overall information security program of the Federal Trade Commission (FTC) at Level 3, "Consistently Implemented." The OIG assessed Privacy Programs at Level 4, "Managed and Measurable".

An IT modernization effort is currently underway. The effort has completed the rewriting of IT and information security policies and procedures to support the authorization of internal and external services for operation or use. Alongside that effort, the FTC has been addressing prior-year recommendations and, in FY 2018, the OIG closed eleven related to IT Governance and eight related to prior FISMA reports. To achieve a Level 4 rating for the overall information security program, the agency should continue the implementation of technical capabilities that enforce its policies in accordance with documentation for systems within its inventory, including system security plans, authorizations to operate, and authorizations to use.

FY 2018 Annual Cybersecurity Performance Summary

General Services Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	5	0	1
E-mail	174	78	5
External/Removable Media	0	0	0
Impersonation	2	NA	0
Improper Usage	58	44	49
Loss or Theft of Equipment	335	230	0
Web	21	6	3
Other	70	76	21
Multiple Attack Vectors	0	1	0
Total	665	435	79

CIO Self-Assessment

The General Services Administration (GSA) aligns its enterprise risk management strategy to the quarterly risk assessment scorecard. Also, in response to the Risk Determination Report, GSA identified three primary risks: lack of hardened security configurations across all systems and devices, lack of privileged two-factor authentication across all systems and devices, and the exploitation of sensitive information through email phishing attacks. During the course of FY18, GSA has taken the following actions to better mitigate these threats:

- deployed Email Threat Prevention (ETP) service across the enterprise to prevent phishing emails from arriving at user's inbox
- deployed Next Generation Antivirus (NGAV) solution, which detects and protects GSA endpoints against malware based on Artificial Intelligence and machine learning
- Continued to deploy "Manage Privileges and Accounts (PRIV)" security capability as part of CDM phase 2 and CDM DEFEND.

GSA is actively working with HVA systems lacking the capabilities of MFA for network/local access to privileged and non-privileged accounts, encrypting data at rest, and having a central flaw remediation solution and formulating plans to address these risks.

Independent Assessment

The information security program of the General Services Administration was evaluated as not effective, as not all cybersecurity functions were evaluated as Managed and Measurable. Consistent with applicable Federal Information Security Modernization Act requirements, OMB policy and guidelines, and NIST standards and guidelines, GSA has consistently implemented its information security program and practices (policies, procedures, and tools) for the five cybersecurity functions and eight FISMA program areas. We identified eight deficiencies within three of the five cybersecurity functions and four of the eight FISMA metric domains based on a selection of six federal and two contractor information systems, entity wide testing, and follow-up on prior year recommendations. We do note that GSA has implemented CDM tools and CMaaS (ForeScout Agent Secure Connector, BigFix, Tenable, Splunk, and Archer). GSA is the process of designing and operationalizing the reports and dashboards that will be available to information system security managers (ISSMs), information system security officers (ISSOs), Office of Chief Information Security Officer (OCISO), and other senior management.

FY 2018 Annual Cybersecurity Performance Summary

Gulf Coast Ecosystem Restoration Council

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

Gulf Coast Ecosystem Restoration Council (Council) is a small Federal Agency tasked with developing and implementing a comprehensive plan to restore the ecosystem and the economy of the Gulf Coast region. As such, the Council partners with local, state, and federal agencies to accomplish this goal. The Council uses IT to develop key collaboration tools and maintain a dynamic environment that fosters productive relationships with our partners. The Council strives to ensure a FISMA compliant IT infrastructure that allows the Council to perform its activities in a secure manner.

As a small agency, the Council's risk management strategy is to partner with other Federal agencies to leverage the use of their shared services and IT security infrastructure. This methodology allows for efficient use of IT budget; allowing the Council to focus on its core mission. The Council still plays an active part in assessing the IT services for security and developing policy and procedures concerning controls defined within the Risk Management Framework.

The Council only has a single system consisting of endpoint devices that provides connection to our Federal Shared Services partners. This system by default was designated as HVA. This past fiscal year the Council has worked hard to ensure its IT infrastructure meets federal guidelines. This includes implementing a secure TIC for the agency to include implementing all three of the Einstein levels. In addition, the Council has put in a place a contracted vendor to provide patch management and malware scanning on a recurring basis. The Council is working with the CDM program office to implement CDM. Overall the Council's information assurance program is effective and meeting the targeted security goals.

Independent Assessment

The information security program of the Gulf Coast Ecosystem Restoration Council was evaluated as effective. Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and have been maintained for the 5 Cybersecurity Functions and 8 FISMA Metric Domains. RMA Associates, LLC found that the Council's information security program and practices were effective for the period July 1, 2017 through June 30, 2018.

FY 2018 Annual Cybersecurity Performance Summary

Institute of Museum and Library Services

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

IMLS has a similar risk profile to other small, internet-enabled organizations that have had significant success adopting cloud-based services. IMLS has aligned its IT strategy with OMB and the President Management Agenda's focus on utilizing interagency shared services, cloud SaaS and IaaS models, and other ways to reduce the agency's local directly-administered footprint in order to minimize the risk exposure introduced by the limited resources of being a small agency. By utilizing the world-class security, automation, patch management, and monitoring tools of our interagency and commercial partners, IMLS has significantly strengthened its overall information security posture.

To support and enable this transition, in FY2018 the IMLS Risk Management Council undertook a function-wide IT risk assessment to identify projects to mitigate key risks across the CIO function. The CIO established a portfolio of high risk mitigation projects to conduct across FY2018-2020.

During FY2018, major improvements came from completing highlighted projects in configuration management and endpoint protection, extending that protection to all agency-issued mobile devices, agency-wide information system inventory and enterprise data inventory to link categorization and procedures, configuration baseline of the full agency infrastructure following cloud migration, full patch management across the agency infrastructure, and review/update of core information security and IT management policies and procedures.

A major focus in FY2019-FY2020 is the migration from the decades old legacy grants management system to a new interagency shared service; this grants management system is the sole critical agency system managed locally and is the principal reason the IMLS GSS is designated as its sole HVA.

Independent Assessment

The information security program of the Institute of Museum and Library Services was evaluated as effective. It is the independent assessor's professional opinion based on the results of the security assessment, that IMLS has complied with the majority of security control requirements tested during the security assessment of the IMLS GSS. However, certain discrepancies and process improvements are required to be corrected and implemented by the IMLS Information Security Team in the following areas:

- IMLS enforces the acknowledgement of access agreements, which include nondisclosure agreements (NDA), acceptable use agreements, Rules of Behavior (RoB), and conflict-of-interest agreements. The existing RoB does not require a signature nor does IMLS require annual revalidation.
- IMLS has policies in place that discuss the desired behavior and treatment of PII, including the prohibition of saving PII on desktops and local drives. While a policy is in place IMLS has not implemented technical mechanisms to prevent users from saving PII locally.
- Information System Contingency Plan testing and exercises have been defined and include, notification procedures and system recovery from backup. However, IMLS has not conducted contingency plan tests against the documented procedures.

FY 2018 Annual Cybersecurity Performance Summary

Inter-American Foundation

Framework	CIO Rating	IG Rating
Identify	At Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	1	0	0

CIO Self-Assessment

As part of the annual OIG FISMA audit, it was concluded that the Inter-American Foundation (IAF) generally complied with FISMA by implementing 63 of 72 security controls reviewed for selected information systems. The controls are designed to preserve the confidentiality, integrity, and availability of the Foundation's information and information systems. Among the controls IAF effectively implemented were the following:

- Change management policy and procedures.
- Procedures for security awareness and training.
- Information system continuous monitoring.
- Account management procedures for bringing on new employees and ensuring terminated employees' access is removed timely.

In addition, the IAF:

- Documented and tested the Incident Response Plan policy.
- Migrated its only HVA system to a FedRAMP cloud environment. The IAF also moved enterprise email to the cloud in 2014. The IAF plans to relocate the COOP physical site to a cloud site, such as AWS, Azure or GCP, by 2019.
- Is implementing continuous monitoring via DHS' CDM program, which is expected to be deployed in FY19.

Recommendations identified from FY18 audit include:

Recommendation 1. Develop and implement an enterprise risk management policy.

- The IAF will develop an updated enterprise risk management policy and procedures consistent with federal requirements and the agency's risk strategy.
- The IAF will annually review and adjust the risk profile with inputs taken from assessments and other defined indicators of risk.

Recommendation 2. Create a change control board or related oversight body that reviews, approves, and manages changes to configuration items; and develops a configuration management

Carry forward Recommendation identified from FY16 audit includes:

Recommendation 7. Implement multi-factor authentication for all network accounts and document the results. The IAF will implement PIV by FY19.

Independent Assessment

The information security program of the Inter-American Foundation was evaluated as effective. IAF's information security program was evaluated as part of the FY 2018 FISMA Audit. This audit included an evaluation of IAF's sole internal information system and for two of nine external systems. The FY 2018 audit noted that 63 of 72 selected NIST SP 800-53, Revision 4, security controls were properly implemented. This led to the determination of IAF having an overall effective information security program. There were four recommendations made to help IAF improve their information security program. The recommendations can be found in the FY 2018 FISMA Audit report.

FY 2018 Annual Cybersecurity Performance Summary

International Boundary and Water Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Managed and Measurable
Detect	At Risk	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	1

CIO Self-Assessment

The International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC) consists of 1 moderate GSS and 2 high Supervisory Control and Data Acquisitions (SCADA) operational systems. All information security programs comply with laws and regulation established by FISMA, as amended, and standards prescribed by the OMB and NIST. The IBWC completed all requirements related to BOD 18-01, prioritizing the importance of DMARC, Sender Policy Framework (SPF), STARTTLS, HTTPS and HTTP Strict Transport Security (HSTS) on agency internet facing servers. The IBWC also migrated a legacy Novell GroupWise Email Server to a more secure FedRAMP compliant Office 365 Exchange system. During FY 2018, the IBWC also reauthorized continued operation of the General Support System.

Independent Assessment

The information security program of the International Boundary and Water Commission was evaluated as effective. OIG found that USIBWC generally implemented an effective information security program that supports the operations and assets of USIBWC. However, OIG noted deficiencies that require remediation for USIBWC to fully comply with FISMA. OIG identified issues related to the risk management, configuration management, identify and access management, and information security continuous monitoring domains.

FY 2018 Annual Cybersecurity Performance Summary

International Trade Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Managed and Measurable
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	3	0	1
Loss or Theft of Equipment	0	0	1
Web	3	0	0
Other	2	3	2
Multiple Attack Vectors	1	0	0
Total	9	3	4

CIO Self-Assessment

USITC has reviewed its assets and mission functions and has determined that it does not currently possess any “assets, systems, and data that are of particular interest to potential adversaries” (HVA) or any mission functions that cannot be deferred during an emergency or disaster (MEF). Following USITC’s strategy and approach to managing enterprise risk has identified the following overarching cybersecurity risk categories currently being tracked and managed within the Commission’s Enterprise Risk Management program.

IT Staffing—The Commission has had difficulty filling highly skilled technical positions (networking, software development, and cybersecurity), even with contractors. The commercial sector can afford higher salaries for the best talent. Another risk results from the Commission’s inability to host TS-SCI clearances required by OMB M-16-03 which allow senior cybersecurity staff to review classified threat feeds.

System Authorizations—Not all of the Commission’s systems have ATOs. Of the three defined system boundaries, two are authorized, and one is going through the security control assessment process.

Data Center / Hardware / Software—USITC Headquarters data center lacks redundant local loop communication circuits and the building’s electrical and HVAC systems cannot support a modern data center. The Commission also has a few hardware and software platforms that have reached end of life.

Recovery planning—The Business Impact Analyses (BIAs) for the Commission’s mission functions are in the nascent stage. Since BIA priorities flow down and inform disaster recovery planning, contingency planning, and testing, the Commission has near and mid-term work items to resolve to adequately address the cybersecurity framework Recover function.

Independent Assessment

The information security program of the International Trade Commission was evaluated as effective. The Commission enforces application control across all compatible devices for user's desktop and laptop devices. This means that the Commission has good control of the software on its network. And controls configurations of its devices.

The Commission has a robust vulnerability identification and remediation program. Which means that the Commission has good control of the hardware on its network.

FY 2018 Annual Cybersecurity Performance Summary

Japan-United States Friendship Commission

Framework	CIO Rating	IG Rating
Identify	High Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Japan-United States Friendship Commission has implemented industry standard safety procedures to mitigate risks and to ensure that data is protected.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Japan-United States Friendship Commission was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Japan-United States Friendship Commission will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Marine Mammal Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Optimized
Protect	At Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Optimized
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Marine Mammal Commission is a micro agency consisting of three Commissioners and nine members of the Committee of Scientific Advisors on Marine Mammals, all of who are special government employees, supported by a staff of 14 full-time government employees.

The Marine Mammal Commission does not own or manage any information systems. Any Personally Identifiable Information is collected only for necessary purposes and is secured.

The main means of ensuring security of federal information are as follows:

1) The Commission does not originate, receive, or store classified information, either electronically or in hard-copy. The Commission has a suitably rated safe that is kept in a locked room for storing such information, if the need should arise.
2) The Commission's official personnel records are maintained by the General Services Administration, Commissions and Boards. Supervisor records are maintained in a locked metal cabinet in the office of the Commission's Chief Administrative Officer. The Chief Administrative Officer and the Executive Director are the only staff with access to those records.
3) In FY 2012 the Commission initiated the Managed Trusted Internet Protocol Service (MTIPS) to provide a Trusted Internet Connection (TIC). The Commission has signed the EINSTEIN Memorandum of Agreement with the Department of Homeland Security.
4) All agency computers have antivirus software installed.

Independent Assessment

The information security program of the Marine Mammal Commission was evaluated as effective.

FY 2018 Annual Cybersecurity Performance Summary

Merit Systems Protection Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Ad Hoc
Detect	At Risk	Defined
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	3	8
Loss or Theft of Equipment	0	2	2
Web	0	1	0
Other	3	2	0
Multiple Attack Vectors	0	0	0
Total	3	8	10

CIO Self-Assessment

The Merit Systems Protection Board (MSPB or Board) will install CDM equipment in coordination with DHS in November 2018 as one of the Wave 5 agencies.

In addition, the Board completed all but two of the DHS BOD 18-01 requirements before October 16, 2018, including setting the DMARC email policy to "reject". The two remaining tasks are incomplete due to vendor constraints, of which DHS is aware. For one of those tasks DHS provided MSPB with a temporary exception until it is resolved.

The Board also implemented the DHS-sponsored Traffic Aggregation service in February 2018. This is the third protection MSPB implemented in conjunction with AT&T's Managed Trusted Internet Protocol Service. The other protections, Domain Name System Sinkhole and Malicious Email Filtering, were implemented in FY 2017. The Board tested two-factor authentication for its Microsoft Office 365 cloud environment in FY 2018, and will implement it agency-wide in FY 2019.

Independent Assessment

The information security program of the Merit Systems Protection Board was evaluated as not effective. The scope of the audit covered the MSPB GSS. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of each of the IG security domains, and other supporting documentation as it pertains to the MSPB GSS. The results of the assessment were used to measure the maturity of the agency's information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels on which MSPB develops sound policies and procedures, and the advanced maturity levels, so the agency can institutionalize those policies and procedures at the highest level possible.

Upon completion of the audit it is apparent that MSPB has put forth a concerted effort in securing the organization GSS environment. It is ISSLoB's professional opinion based on the results of the security assessment, MSPB has complied with many of the security control requirements tested during the security assessment of the MSPB GSS. However, certain discrepancies and process improvements are required to be corrected and implemented by the MSPB Information Security Team in the following areas:

1) MSPB is either lacking or has not finalized the following documentation: an Access Control Policy and ICAM Strategy, Risk Management Policy or procedures, Security Awareness Policy and a Training Strategy or plan, and an Incident Response Policy.
2) MSPB has implemented secure configurations. However, MSPB does not follow the NIST guidance on secure configuration settings.
3) MSPB has privacy roles and provides privacy training to users. However, the agency needs to develop a more in-depth program to ensure the protection of data that is collected, used, maintained, shared, and disposed of by its information systems.

FY 2018 Annual Cybersecurity Performance Summary

Millennium Challenge Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	0	1
External/Removable Media	1	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	13	15	0
Web	2	2	1
Other	7	9	0
Multiple Attack Vectors	0	0	0
Total	24	26	2

CIO Self-Assessment

The Millennium Challenge Corporation (MCC) has complied with the email security goals of BOD 18-01, and is working to resolve the web security portion by leveraging the President's Management Agenda on Federal IT Modernization and Cloud Smart goals in order to migrate non-compliant systems to modern, compliant, cloud-hosted systems for full implementation of the web portion.

In addition, MCC's chief risk officer will ensure that its MCC Integrated Risk Management Framework document (which will include documentation of the implementation of its Enterprise Risk Management program) includes its strategy to manage risks associated with the operation and use of information systems by June 30, 2019.

MCC's Domestic & International Security Office will update and provide the Personnel Security Policy, which includes the Background Investigation and Clearances for Federal Employment, Contract Service and/or Volunteer Service by December 31, 2018.

MCC Domestic & International Security will document and implement a manual process that validates the completeness and accuracy of the existing Access-based Security Database with a long-term goal of implementing a system to perform the process. MCC will provide a formal management decision no later than March 29, 2019.

Lastly, MCC Domestic & International Security will document and implement a manual process that tracks reinvestigation of employees and contractors in a timely manner with a long-term goal of implementing a system to perform the process. MCC will provide a formal management decision no later than March 29, 2019.

Independent Assessment

The information security program of the Millennium Challenge Corporation was evaluated as effective. MCC's information security program was evaluated as part of the FY 2018 FISMA Audit. This audit included an evaluation of four out of seven FISMA reportable systems at MCC. The FY 2018 FISMA Audit noted 66 of 74 selected NIST 800-53, Revision 4 security controls were properly implemented. This led to the determination of MCC having an overall effective information security program. There were several recommendations made to help MCC improve their information security program.

FY 2018 Annual Cybersecurity Performance Summary

Morris K. Udall Foundation

Framework	CIO Rating	IG Rating
Identify	High Risk	NA
Protect	High Risk	NA
Detect	At Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	High Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

In 2018 the Morris K. Udall Foundation maintained the cybersecurity standards established in previous years.

As the Foundation does not participate in the DHS' CDM program, purchasing and implementing equivalent controls have been both cost and time prohibitive.

Upgrades in 2018 to perimeter firewalls have improved network security from outside access. In addition, steps to comply with BOD 18-01 have further improved security posture. The Foundation plans to implement two-factor authentication using PIV cards in 2019.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Morris K. Udall Foundation was not performed for FY 2018, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Morris K. Udall Foundation will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

National Aeronautics and Space Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	7	7	2
E-mail	99	646	5
External/Removable Media	11	3	0
Impersonation	5	NA	0
Improper Usage	141	209	180
Loss or Theft of Equipment	427	249	23
Web	678	354	30
Other	39	333	76
Multiple Attack Vectors	77	46	1
Total	1,484	1,847	317

CIO Self-Assessment

NASA is required to and responsible for ensuring information technology's secure use in support of its mission objectives. A resilient cyber posture requires strong cyber hygiene practices to effectively identify, protect, detect, respond, and recover from cyber events that introduce risk. Cybersecurity and Mission/Project teams must collaborate to integrate cybersecurity principles in the risk management discipline. The Agency is working to integrate cybersecurity into all that everything the agencies does by engaging in crosscutting activities to update policies and practices.

NASA has made significant improvements by deploying and maturing cybersecurity capabilities in support of a more resilient cybersecurity posture. This includes continued deployment of continuous monitoring capabilities via the CDM Program across Corporate and Mission environments. CDM enables NASA to identify critical vulnerabilities for remediation on its Corporate IT assets, with full Mission deployment anticipated in Q2FY19. Additionally, NASA exceeded a Federal target of achieving strong authentication for 85 percent of unprivileged user accounts, reaching 87 percent in Q4FY18. NASA also recently signed the Unauthorized Devices (UD) memo, a cornerstone of its Strategy to Improve Network Security. Together, CDM tools, UD policy, and Network Access Control tools being deployed in Q1FY19 will enable NASA to identify, monitor, and technically block unauthorized devices from connecting to NASA's internal networks. Additionally, NASA is in the process of finalizing the measurement methodology and capability to measure HVA machines for user based enforcement or machine based enforcement; which will improve NASA's HVA reporting by Q1FY19.

Independent Assessment

The information security program of the National Aeronautics and Space Administration was evaluated as not effective. During our FY 2018 review, the OIG assessed NASA's information security policies, procedures, and practices by examining seven (7) information systems. Further, the OIG assessed the Agency's overall cybersecurity posture utilizing a variety of techniques that leveraged prior work performed by NASA, NASA OIG, and GAO. The OIG also evaluated NASA's progress in addressing deficiencies identified in prior FISMA and information security reviews. Cumulatively, those assessments assisted us in reaching our conclusions. By implementing previous audit recommendations and implementing corrective actions, NASA continues to improve its overall cybersecurity posture.

However, as indicated by the results of this review, information security continues to remain a significant challenge for NASA in addressing considerable cybersecurity gaps and in its efforts to address cyber threats in an evolving threat landscape. While NASA continues to make progress in securing its networks and information systems, they remain vulnerable to cybersecurity threats.

FY 2018 Annual Cybersecurity Performance Summary

National Archives and Records Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Ad Hoc
Detect	At Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	2
Loss or Theft of Equipment	0	0	0
Web	1	6	2
Other	28	71	4
Multiple Attack Vectors	0	1	0
Total	30	80	8

CIO Self-Assessment

NARA information security policies, procedures, and practices provide adequate protections that are generally effective. However, in some cases we lack the formal documentation necessary to ensure that our policies and strategies are consistently implemented. Because of long standing risks in NARA IT security, the CIO declared IT security a material weakness in internal controls in FY 2015 – FY 2018.

NARA continues to improve its ability to protect the confidentiality, integrity, and availability of NARA resources. In FY 2018, the DHS performed a RVA and a SAR of the agency's HVAs, resulting in the identification of weaknesses in NARA's HVA environment. This effort is a high priority for the Agency and NARA has funded additional resources, namely a dedicated ISSO and Security Engineer, to remediate residual weaknesses for HVA's.

In FY 2018, NARA was able to successfully implemented agency-wide mandatory use of PIV for network access for all network users, along with ensuring all mobile assets have the ability to remotely wipe agency data. In addition, NARA acquired a new contract which provides dedicated resources with the goal of improving agency moderate impact system ATO's throughout FY 2019.

Independent Assessment

The information security program of the National Archives and Records Administration was evaluated as not effective. NARA has continued to make progress on several fronts, including the communication of the CFM to key stakeholders during FY 2018 and the procurement of a new contract to obtain ISSOS during the latter part of FY 2018. However, there are still concerns about the effectiveness of NARA's information security program, such as the absence, turnover, and management of ISSOs. In addition, the organization structure of the CIO remains challenged as the CIO does not report directly to the Archivist.

To improve the accuracy of inventory reporting for all its systems and components, and to ensure appropriate security control assessments and authorizations of these systems are implemented and updated, NARA needs to continue identifying systems on its network and those systems not connected to the network but under the management and responsibility of NARA. NARA must conduct security assessments and proceed through the authorization process including development of security assessment packages for all major applications. NARA should work to improve its contingency planning function to ensure it completes, updates, and tests its system-level contingency plans, conducts system BIAs, and documents all implementation details within its SSPs.

Finally, NARA continues to stress their commitment to improving information security throughout the Agency and will continue to work with the OIG to ensure information security weaknesses are adequately addressed. The content of this narrative was shared and discussed with NARA's Office of Information Services.

FY 2018 Annual Cybersecurity Performance Summary

National Capital Planning Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	4	1
Multiple Attack Vectors	0	0	0
Total	1	6	1

CIO Self-Assessment

In Fiscal Year 2018, the National Capital Planning Commission (NCPC) made significant improvement to its security posture by segmenting its network and applying firewall rules between segments to control the flow of information. The NCPC IT team also configured existing security automation tools to monitor and alert the team upon potential events and incidents. The team continues to fine tune existing security tools to ensure they provide valuable information to monitor and respond to events.

The IT team and web developers worked collaboratively to meet the requirements in BOD 18-01, Enhance Email and Web Security. The team continues to work on resolving DMARC policy requirements. Tests have shown that a significant number of agency announcements would not be delivered to recipients if DMARC policy is set to reject. The team has engaged vendor support and reached out to the DHS FNR BOD team for assistance.

NCPC reported two HVAs in response to BOD 18-02, Securing High Value Assets. These two systems are critical in supporting the mission of the agency and both have received an ATO. Specifically, the team is working to address concerns with configuration management, patch management, and securing remote access mechanisms.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the National Capital Planning Commission was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The National Capital Planning Commission will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

National Council on Disability

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	Managing Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	0	1	0

CIO Self-Assessment

National Council on Disability completed an on-site physical and environment assessments of data center facility, vulnerability assessments and reviews, system security documentation assessments, interviews with key personnel.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the National Council on Disability was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The National Council on Disability will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

National Credit Union Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	11	3
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	5	7
Loss or Theft of Equipment	1	9	21
Web	0	3	7
Other	1	6	4
Multiple Attack Vectors	0	1	0
Total	4	35	42

CIO Self-Assessment

The National Credit Union Administration (NCUA) Office of the Chief Information Officer (OCIO) continues to improve the effectiveness of the information security program and will continue to strengthen the consistent implementation of policies, procedures, and strategies in 2019. While we made progress in 2018, the following key risk areas remain the most significant:

1) Data Management Security: The NCUA has established an Enterprise Data Reference Model (DRM) and has staffed an Enterprise Data Program to promote the accuracy, accessibility, consistency and security of our agency's data. The initial focus of the Program is on a subset of the agency's data domains and will expand to other domains as the management of data matures. While the NCUA has made progress, there is still risk to the agency's protection of data holdings as the program is in its early stages;

2) Legacy Application Security: The NCUA conducted an assessment of legacy application code to identify vulnerabilities and continues to analyze the feasibility of repairs or compensating controls for legacy systems. The NCUA's enterprise business system modernization is underway with a 5-year road map to retire legacy applications beginning in 2020;

3) USB/Whitelisting for the NCUA Examiners: In 2018, the NCUA issued FIPS 140-2 encrypted external hard drives to all the NCUA Examiners, installed a USB management capability on all agency assets, and issued guidance for all credit unions to utilize one of our approved methods to securely transfer data. The NCUA will implement the USB restrictions and whitelisting in 2019; and

4) High Value Assets: The NCUA completed risk assessments on its HVAs in 2018. In conjunction with the risk assessments, the agency has improved capabilities in the area of threat detection, data protection and incident response using a two-pronged approach of personnel and technology.

Independent Assessment

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) evaluated the NCUA's information security program as effective. We assessed the NCUA in all Function areas and underlying Domains identified in the FY 2018 IG FISMA Reporting metrics as they pertain to the NCUA's six FISMA reportable systems and its overall information security program.

The NCUA has continued to strengthen its information security program during FY 2018. Specifically, we determined the NCUA has effective access controls and is effective in its security awareness and training program, its contingency planning and in its privacy and data protection. In addition, the NCUA addressed and closed: (a) the last six remaining recommendations from our FY 2016 FISMA report; and (b) seven of the eight recommendations from the FY 2017 FISMA report. Furthermore, the NCUA is in the process of addressing and resolving the one remaining recommendation from the FISMA 2017 report. The NCUA's appetite for technology and information management risk is low with regard to cost-effective security, as the confidentiality, integrity and availability of systems, data and information is foremost. Although we identified areas for improvement this year in the areas of information security continuous monitoring, configuration management, personnel security, and risk management, considering the compensating controls in place, we deemed NCUA's overall information security program effective. We made 10 recommendations, which should help the NCUA continue to improve the effectiveness of its information security program. We included these recommendations in the OIG's FY 2018 FISMA report.

FY 2018 Annual Cybersecurity Performance Summary

National Endowment for the Arts

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	1
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	1	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	2	1	1

CIO Self-Assessment

During this reporting period, a detailed assessment of the adequacy and effectiveness of the Agency's information security policies, procedures, practices and progress towards meeting the FY18 government-wide targets in the CAP Goal metrics was performed. The result was the development, training, implementation and institutionalization of 18 required security policies and procedures per NIST 800-53 Rev4, 800-39, and FIPS 200 and 201.

The Agency conducted a series phishing exercises, human firewall training, penetration testing, and used an automated security awareness program to expand the reach of the cybersecurity program. We used the artificial intelligence part of the tool to determine the vulnerability level of your network by giving you an indication of how many people may be susceptible to an email-born social engineering attack. The NEA score 3.4% as being phishing-prone compared to the industry benchmark of 29.3%.

Independent Assessment

The information security program of the National Endowment for the Arts was evaluated as not effective. The National Endowment for the Arts (NEA) Office of Inspector General (OIG) contracted with an independent assessor to determine the effectiveness of NEA's information security program and practices in fiscal year (FY) 2018. Overall, NEA has made progress in addressing previously identified information security deficiencies. For example, NEA developed baseline policy related to each IG FISMA metric domain. However, the independent assessor has determined that NEA's information security program still needs improvement to become effective. The independent assessor has identified weaknesses in all IG FISMA metric domains, and recommends NEA continue to improve the information security program and accordingly has provided recommendations for each IG FISMA metric domain.

FY 2018 Annual Cybersecurity Performance Summary

National Endowment for the Humanities

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Managed and Measurable
Detect	At Risk	Defined
Respond	At Risk	Consistently Implemented
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	1	0	0
E-mail	1	1	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	1	3
Web	0	0	0
Other	4	0	0
Multiple Attack Vectors	0	0	0
Total	6	2	3

CIO Self-Assessment

The National Endowment for the Humanities (NEH) has made significant improvements to its cybersecurity, including security related to two systems identified as HVAs. The agency has addressed nearly all major risks identified in the 2017 report, noting the following successes and remaining risks:

- Two remote access systems (one for email and one for full teleworking capabilities) now require two-factor authentication.
- The website has been updated to the latest version of Drupal and is fully patched to the latest stable version.
- NEH has contracted with its MTIPS provider to use DNSSEC.
- Continuous Diagnostics and Monitoring is not fully in place. The Agency is working closely with DHS who will be rolling out CDM during FY19 (part of the TO2F group).
- NEH now has a full-time CISO, a dedicated cybersecurity staff member.
- Among other tasks, the CISO will be working on new ISCM and contingency plans for our HVAs and has put a plan in place to update all A&As, including for our HVAs.

The Agency has also been performing a number of system reviews, including a review of various system ATOs and a review of our anti-phishing training program. The IT team has also been working closely with the agency's COOP team to discuss Mission Essential Functions and how to perform them during a COOP situation. The CIO continues to meet monthly with the agency's Senior Deputy Chairman which has enabled us to secure funding.

Independent Assessment

The information security program of the National Endowment for the Humanities was evaluated as effective. The NEH information security program has been designed to comply with NIST and FISMA requirements. Considering the small size of the Agency, certain activities comprising the information security program are effective in providing continuous visibility into threats and risks to NEH information systems and data.

However, budgetary constraints and competing priorities for agency IT staff have presented challenges in the Agency's ability to fully implement core elements of ISCM and contingency planning. Consequently, the overall effectiveness of the NEH information security program is weakened.

Over the past year, the Agency has undertaken efforts to specifically address weaknesses concerning information security policies, procedures, and practices, as identified during previous FISMA evaluations. Particularly, in August 2018, the Agency hired a CISO to oversee the Agency's cybersecurity program and activities.

FY 2018 Annual Cybersecurity Performance Summary

National Labor Relations Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	1	0
Other	0	0	2
Multiple Attack Vectors	0	1	0
Total	0	2	2

CIO Self-Assessment

The Agency IT Financial Audit determined a weakness in the lack of a contingency plan and testing and IT Security Assessment for the LAN/WAN. The Agency developed and implemented the NLRB LAN/WAN contingency plan and conducted a Contingency and Incident Response Tabletop Exercise facilitated by the DHS NCCIC. In addition, the Agency obtained an independent assessor (DOI Shared Service Center) to test and validate the LAN/WAN SSP in accordance with NIST 800-53A revision 4, which is the Agency's only HVA.

Independent Assessment

The information security program of the National Labor Relations Board was evaluated as not effective. The Agency's information security program was deemed "not effective" because 37 of the 59 metrics were at the "Ad Hoc" or "Defined" level and 2 of the 5 security functions were calculated at the "Ad Hoc" or "Defined" level. However, despite ratings, the NLRB has made improvements from the prior years' assessments.

FY 2018 Annual Cybersecurity Performance Summary

National Mediation Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The National Mediation Board (NMB) has made progress this year in implementing parts of BOD 18-01 and BOD 18-02. The Board is evaluating products for DMARC capabilities, targeting a decision in November 2018 and is sending DMARC information to NCCIC. The Board has implemented https for two HVA case management systems and developed a new website compatible with BOD 18-01, but is awaiting management approval to deploy the site. The Board procured products for phishing and security awareness training. In FY2018, the Board implemented E3A email filtering. As a FISMA Low FIPS-199 categorization for our information, the Board performed an internal Annual Security Assessment and three internal quarterly assessments in FY 2018.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the National Mediation Board was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The National Mediation Board will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

National Science Foundation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	2	0
E-mail	6	5	2
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	1	15	3
Other	20	11	1
Multiple Attack Vectors	0	0	0
Total	27	33	7

CIO Self-Assessment

The National Science Foundation (NSF) has established a strong and comprehensive IT Security Program that is consistent with Government-wide guidance and patterned after industry best practices. NSF maintains a balanced approach to IT security where risk is assessed, understood, and mitigated appropriately. Protecting information is vitally important to NSF's mission; therefore, NSF concentrates on areas with increased risk and takes prudent steps to mitigate the risk. Along with risk management, NSF continues to proactively assess, monitor, and enhance the maturity of the IT Security Program to improve the overall effectiveness of NSF's security posture.

NSF maintains a HVA inventory based on its Mission Essential Functions related to grants management and merit review systems. NSF's major systems contain PII and comprise the inventory of systems on NSF's network. NSF continued to implement additional controls in areas such as anti-malware, user access provisioning, and audit log monitoring in FY 2018.

NSF continued a continuous monitoring approach that assesses the security state of information systems based on FISMA security requirements and NIST Cybersecurity Framework guidance. NSF conducts continuous enterprise network monitoring, which allows real-time visibility into threats and real-time security status of agency systems.

Independent Assessment

The information security program of the National Science Foundation was evaluated as effective. In order to assess how the National Science Foundation (NSF) established its agency-wide Information Security Program and practices as required by FISMA, an independent assessor performed detailed testing of NSF's Network General Support System (GSS), iTRAK application, Awards application, and eJacket application for compliance with selected National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4 controls. Overall, the Information Security Program was rated positively. The OIG concluded that NSF has successfully addressed all cybersecurity findings from FY 2017.

FY 2018 Annual Cybersecurity Performance Summary

National Transportation Safety Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	1	0
Multiple Attack Vectors	0	0	0
Total	2	1	1

CIO Self-Assessment

The National Transportation Safety Board's (NTSB) recent external network upgrade replaced the existing legacy infrastructure, enhanced the NTSB security posture and laid a solid operational foundation. This project removed all legacy end of life network equipment from the external infrastructure thereby significantly reducing risks and enhancing our boundary protection. Also NTSB completed the PIV deployment and established a new SOC to monitor security posture of NTSB infrastructure. The SOC was provided with packet, flow and log analysis (SIEM) systems to provide enhanced cyber situational awareness.

Furthermore, NTSB deployed a zero trust remote access computing platform to reduce remote access based threats to NTSB infrastructure. Also NTSB deployed a web security gateway which provides web content filtering and SSL inspection of all outbound web traffic. The HVA servers reside in the GSS boundary and inherits all new security controls we have deployed.

Independent Assessment

The information security program of the National Transportation Safety Board was evaluated as effective. The scope of this audit covers the NTSB GSS. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of each of the IG security domains, and other supporting documentation as it pertains to the NTSB GSS. NTSB has gone through extensive efforts in securing the organization GSS environment and has complied with most security control requirements tested during the security assessment of the NTSB information security program and NTSB information systems.

The NTSB information security program was found to be implemented effectively due to the following factors validated by operational evidence: Development and dissemination of policies and procedures according to security control criteria requirements, Effective ISCM program, Effective Configuration Management program, Automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, ISCM, and Configuration Management programs, Security training is monitored and provided ,effective Incident Response program, established and defined a Contingency Planning program.

The recommendations included completion of DHS CDM program implementation and develop, define, implement, and disseminate a business impact analysis.

FY 2018 Annual Cybersecurity Performance Summary

Nuclear Regulatory Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	1	3	0
External/Removable Media	0	0	0
Impersonation	0	NA	2
Improper Usage	7	12	0
Loss or Theft of Equipment	2	1	0
Web	0	0	0
Other	14	23	0
Multiple Attack Vectors	1	1	0
Total	25	40	2

CIO Self-Assessment

FY2018 cybersecurity risks affecting the IT systems that support the US Nuclear Regulatory Commission's HVAs and Mission Essential Functions include exploitation of unpatched software security vulnerabilities, exploitation of software vulnerabilities in unsupported software and operating systems for which vendor patches are no longer available, and advanced persistent threat (APT) attacks by adversaries. Actions taken to mitigate these risks include: (1) streamlining of processes for deployment of vendor patches so that critical and high vulnerabilities are addressed on agency systems within 30 days; (2) outreach to system owners still using unsupported applications and operating systems like Windows XP and Windows 2003 to provide financial and technical support to ease their transition to modern operating systems like Windows 2016; and (3) implementation of new technologies like Next Generation Anti-Virus (Palo Alto Traps) and a Cloud-based malware execution sandbox (Palo Alto Wildfire) to assist in detection of APT attacks. Review of data from agency security scanning systems during FY2018 show positive results from the mitigations implemented during the past year.

Independent Assessment

The information security program of the Nuclear Regulatory Commission was evaluated as effective. NRC's information security program is effective. NRC has developed and established ERM policies and procedures which provide foundation of NRC's ERM governance and communication structure. NRC has integrated ERM to address the full spectrum of agency's risk portfolio across all its organizational and business aspects. NRC's ERM directive integrates enterprise risk management into the agency's performance management and internal control frameworks to facilitate the improvement of NRC's mission delivery, reduction of costs, and focus on corrective actions of its key enterprise risks.

Additionally, NRC's continuous monitoring program monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates to continuously improve its ISCM program. NRC has updated its Cybersecurity Risk Dashboard to include ATO, Continuous Monitoring Status Report, BIA, and contingency plan updates for each of NRC's FISMA systems. NRC maintains two separate categories of programmatic POA&Ms, one to address recommendations for the Inspector General and another for issues/findings that cannot be resolved by a single System Owner. All NRC FISMA systems are under an ongoing ATO with an exception of ADAMS, which is still under the periodic ATO. CDM Phase 2 has been completed and CDM Phase 3 is in the process of being implemented. CDM dashboard is scheduled to be operational in FY19.

FY 2018 Annual Cybersecurity Performance Summary

Nuclear Waste Technical Review Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

NWTRB's cybersecurity risks include crimeware, cyber espionage, denial of service, insider / privilege misuse, general errors, physical theft/loss, and web application attacks. Given the dynamic nature of cyber threats and that these threats tend to aggregate into broader groups, the agency focuses risk management efforts on these groups of cyber threats. The agency has and continues to prioritize risk responses based on the probability and impact that a threat event would have on operations. NWTRB's risk response to cybersecurity threats has been to mitigate the risk associated with cyber threats. This has been achieved for the agency's system and HVAs in FY18 through the implementation and continued monitoring of NIST based security controls, user training, security devices, and security services. NWTRB has actively taken advantage of E3A offerings, having successfully onboarded with the DNS Sinkhole Service (DSS), Malicious Email Filtering (MEF), and the Intrusion Prevention Security Service (IPSS). The agency has continued to work with DHS to protect federal systems having completed the tasks associated with the 18-01 and 02 Binding Operational Directives and resolved vulnerabilities related to events such as the Meltdown/Spectre vulnerabilities. Further, NWTRB has maintained internal systems over FY18 to ensure that critical and high risk CVEs have been resolved within 14 days. The results of a third-party audit conducted on agency systems concluded with 0 high risk findings.

Independent Assessment

The information security program of the Nuclear Waste Technical Review Board was evaluated as effective. NWTRB is a micro agency with limited manpower and budget. As a result the agency utilizes risk-based determinations using the FIPS 199 system classification (which is low) to best decide on how resources are spent in the protection of assets. The agency is currently focused on achieving a fully Defined maturity level across all function areas as a baseline.

The agency was able to meet the Defined maturity level or better in seven of eight function areas. Of the thirteen findings identified by the assessment, there were no High Risk findings, with six Low Risk and seven Moderate Risk. These findings and associated recommendations were developed into POA&Ms for remediation in FY19. Moving forward NWTRB will seek to further improve through the maturity model levels as appropriate in consideration of agency constraints and risk.

FY 2018 Annual Cybersecurity Performance Summary

Occupational Safety and Health Review Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	At Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The FY 2018 independent audit demonstrates the Review Commission's commitment to keeping up with additions and changes to FISMA law. Some specific examples in recent years include the incorporation of NIST Special Publication 800-53 Revision 4, NIST Special Publication 800-18, Federal Information Processing Standards (FIPS) 199, FIPS 200, and FIPS 201, each of which place additional requirements on the agency.

The Review Commission, in accordance with DHS BOD 18-01, "Enhance Email and Web Security", has activated all components defined to ensure the integrity and confidentially of internet-delivered data, minimize spam, and better protect users who might otherwise fall victim to a phishing email that appears to come from a Government-owned system. All Review Commission systems use the HTTP Strict Transport Security, a web policy mechanism that helps protect our website against protocol attacks. This complies with OMB Memorandum 15-13.

The Review Commission's security program continues to be incorporated into its annual performance and security plans in accordance with the law and provides reasonable assurances and safeguards to maintain integrity and competence. Furthermore, the Review Commission practices delegation of authority as a structured organization with defined separation of duties and supervision.

IT personnel have received training on network security, Windows Server 2012 and continuity of operations planning. Most incidents (none in the current FY) that occur are resolved within a few hours, with the results of the incident(s) documented and explained to the users.

Independent Assessment

The information security program of the Occupational Safety and Health Review Commission was evaluated as effective. Review resulted in 12 remediation items included in the POA&Ms for the agency.

FY 2018 Annual Cybersecurity Performance Summary

Office of Government Ethics

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Office of Government Ethics (OGE) budgeted for an IT refresh in FY 2018 to replace major infrastructure components and introduce new technology. For example, OGE is migrating our data center from Virtual Desktop Infrastructure (VDI) to Hyper-Converged Infrastructure (HCI).

However, due to the FY 2018 budget continuing resolution, the procurement process was delayed by several months. This delay resulted in our FY 2018 independent security assessment review being conducted simultaneously with our IT refresh implementation. This will have a negative impact on the "findings" reported by the independent security assessors.

Nevertheless, the OGE is committed to the goal of enhancing its performance security metrics and implementing policies and procedures to protect its IT assets. OGE has taken substantial steps to assess its cybersecurity systems and align its practices to better manage risks.

OGE conducts its risk management process in conjunction with a number of external partners. High and medium risk vulnerabilities are assessed and mitigated in a timely manner, whether identified by an independent security assessment, an eternal partner, or OGE staff. When necessary, OGE implements its risk acceptance process to formally document and justify the acceptance of a known deficiency and the compensating control. OGE requires that a compensating control (or sufficient justification) is defined in order to obtain full approval for a risk acceptance. OGE's risk acceptance process is the result of intense collaboration among the system manager, system administrators and developers, the system owner, the CIO, the authorizing official, and the Senior Agency Official (SAO) for Risk Management.

The OGE Cybersecurity Program provides a level of risk commensurate to the risk as determined by risk assessments conducted by the CIO in collaboration with senior leadership.

Independent Assessment

In FY 2018, the U.S. Office of Government Ethics (OGE) engaged an independent evaluator to assess the status of its information technology cybersecurity program in accordance with NIST SP 800-37 Revision 1, NIST SP 800-53, Revision 4, and NIST SP 800-53A, Revision 4. The independent evaluator identified 62 deficiencies (representing 20% of OGEN security controls). Of the 62 deficiencies identified, the assessor rated 17 as low risk, 44 as moderate risk, and 1 as high risk. Each deficiency has been documented, assigned an ID, and will be tracked until mitigated or accepted by the Authorizing Official (AO). The OGE CIO has written a Plan of Action and Milestones (POAM) document for each deficiency. Each document will be signed by the CIO and the AO to indicate either closure or risk acceptance. However, OGE did not have their independent assessor use IG metrics. Consequently, the IG assessment section is marked "Not Applicable" (NA). The Office of Government Ethics will modify the task order for the FY 2019 independent assessment to include the evaluation of FISMA IG metrics in order to achieve compliance.

FY 2018 Annual Cybersecurity Performance Summary

Office of Navajo and Hopi Indian Relocation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	0	1	0

CIO Self-Assessment

We continually strive to keep up with the necessary securities to keep this agency and our data safe from loss of confidentiality, integrity, and availability. We incorporate, as much as possible, securities recommended from the ISCM program.

Staff view monthly security videos and bi-weekly Phishing tests. For all endpoints the Agency has implemented a new “Next-Generation” antivirus solution, locked down the use of USB flash drives, and mitigated the effects of the Spectre/Meltdown vulnerabilities. The Agency vulnerability scan results continue to be Low (zero).

The FISMA team continues to work with POA&Ms and is progressing in accomplishing the remediation of any weaknesses identified. The Agency has further reduced use of Social Security numbers by transferring 99% client physical files to a NARA records center.

The actions necessary to comply with OMB M-07-16 “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)” have been completed.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Office of Navajo and Hopi Indian Relocation was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Office of Navajo and Hopi Indian Relocation will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Office of Personnel Management

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	Managing Risk	Managed and Measurable
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	13	18	0
External/Removable Media	2	0	0
Impersonation	1	NA	0
Improper Usage	9	38	123
Loss or Theft of Equipment	20	24	8
Web	5	3	1
Other	116	109	28
Multiple Attack Vectors	3	8	0
Total	169	200	160

CIO Self-Assessment

Cybersecurity risks to the Office of Personnel Management (OPM) include the lack of appropriate staffing and maintenance of sufficient resources, specifically related to conducting risk assessments for major information systems, conducting complete and comprehensive tests of security controls, and effectively implementing OPMs Information Security Continuous Monitoring activities.

OCIO is committed to appropriate staffing and maintenance of sufficient resources to support OPM's cybersecurity needs. Senior agency leadership is taking steps to help ensure that critical positions within OCIO are funded and allocated. With this support, the agency is actively interviewing candidates for vacant positions within OCIO and has already extended some offers of employment to fill Information System Security Officer (ISSO) and other roles. OPM has developed an independent assessment team of contractors. The independent assessment team has begun efforts to conduct risk assessments in a consistent manner.

An Enterprise Project Management Office (EPMO) has been established to address a number of agency risks. These include POA&M remediation, enforcement of the System Development Lifecycle policy and maintenance of baseline configurations for all information systems in the agency.

Independent Assessment

The information security program of the Office of Personnel Management was evaluated as not effective. In fiscal year (FY) 2018, the U.S. Office of Personnel Management (OPM)'s overall cybersecurity maturity level is measured as "Defined." This assessment is based on the state of OPM's agency-wide information security program and activities throughout FY2018.

Our audit determined that deficiencies in the agency's information security governance program to be a material weakness in the agency's IT security internal control structure. A lack of resources dedicated to IT operations and the agency's culture of minimizing the role of the CIO are primary factors causing these issues.

This year we have determined that there is a significant deficiency in OPM's security assessment and authorization process. While there appears to be a valid security assessment and authorization in place for almost every major IT system in the agency's system inventory, the quality of the work and supporting documentation is questionable.

FY 2018 Annual Cybersecurity Performance Summary

Office of Special Counsel

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	1	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	1	0	1

CIO Self-Assessment

The Risk Assessment Report (RAR) was conducted by the CISO as a self-assessment of the Office of Special Counsel (OSC). It documents risks to the information system and any vulnerabilities discovered during this internal review of its security control implementation (i.e., existing countermeasures) and security state. It includes a listing of any vulnerabilities that remain after security control implementation, to provide an assessment of the risks associated with the possible exploitation of those vulnerabilities. Furthermore, it provides recommendations for cost-effective solutions that would eliminate or minimize the identified risks for the system.

In FY 2018, OSC strengthened incident response by providing IT security training and bringing awareness to employees. Reviews are performed on a regular basis on activities audit logs, and policies have been configured in Office 365's Security & Compliance module to alert activities that conflicted with those policies.

Additionally, OSC engaged in meaningful cyber situation awareness in network and computing components, threat information, and mission dependencies. Within the first quarter of FY 2019, OSC will have CDM in place. All of these efforts are all in support of OSC's High Value Assets. However, the challenge continues to be budget and IT skills gaps in personnel.

Independent Assessment

The information security program of the Office of Special Counsel was evaluated as effective. DOI Information Shared Service Line of Business performed an evaluation of the effectiveness and level of implementation of security effectiveness as it pertains to the Office of Special Counsel (OSC). The results of the evaluation were used to measure the maturity of the agencies information security processes on a maturity model spectrum developed by DHS and OMB.

The OSC information security program was found to be implemented effectively due to the following factors validated by operational evidence:

• Agency wide policies and procedures have been developed documented and disseminated according to security control criteria requirements;

• Vulnerability scanning of agency information systems and assets has been established and is performed according to FISMA security requirements and frequencies;

• OSC has established an effective configuration management program for its information systems and major applications by employing the use of automated;

• Automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, ISCM, and CM programs;

• OSC ensures that Security training is monitored and provided to OSC stakeholders at least annually and given to OSC personnel according job functions and levels of access;

• OSC has established and maintained an effective IR program; and

• OSC has established and defined a CP program that includes a BIA, CP, and COOP for its main GSS. Additionally, OSC ensures that its contingency program and recovery capabilities are tested at least annually through tabletop exercises of the contingency plan.

FY 2018 Annual Cybersecurity Performance Summary

Office of the Comptroller of the Currency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	2	13
External/Removable Media	0	0	0
Impersonation	0	NA	1
Improper Usage	0	8	0
Loss or Theft of Equipment	0	1	8
Web	0	1	0
Other	0	4	7
Multiple Attack Vectors	0	0	0
Total	0	16	29

CIO Self-Assessment

Key FY2018 risks include: security breaches and cyber exploits caused by personnel error; network exploits caused by unauthorized devices and advanced persistent threats; and mission essential function disruption caused by system failure.

Security breaches and cyber exploits caused by personnel error: Personnel error remains a risk despite OCC technical controls against information loss and malware threats. The OCC addressed this risk by educating its personnel on five cybersecurity risks: information mishandling, secure email failure, device infection, credential loss, and phishing. This effort comprised weekly phishing exercises, with follow-up instruction for 'phished' users, and a new user portal for easy access to instructional materials. A new agency-wide policy addressed remote access to bank networks and examiners managing the available financial supervision information. Training informed supervisory personnel on the policy and related business practices.

Unauthorized devices and advanced persistent threats: The OCC continued installation of CDM Phase 1 tools to further its 24/7 incident monitoring and response capabilities, and is leveraging these tools for better detection and denial of access to unauthorized devices. The OCC also deployed industry-standard Advanced Persistent Threat (APT) technology for real-time APT scanning and alerts; provider's full-scope assessment identified no APT indicators.

Mission essential function disruption: The OCC invested in cyber resilience to address this risk, including an enterprise disaster recovery capability spanning all business and mission-critical applications, and SAN-to-SAN replication to eliminate agency reliance on tape-based recovery. Twelve tests and a full disaster recovery exercise verified OCC capability to continue mission-critical operations.

Independent Assessment

Based on the FY2018 FISMA Reporting Metrics maturity model and direct consideration of the Office of the Comptroller of the Currency (OCC) self-assessment, the information security program of the OCC was evaluated overall as Level 3, Consistently Implemented. This reflects Level 3 or Consistently Implemented assessment in six of the eight IG FISMA Metric domains, and Level 4, Managed and Measurable in two. Per FY 2018 IG FISMA Reporting Metrics instructions, a security program is considered to be effective only if at Level 4, Managed and Measureable, overall.

FY 2018 Annual Cybersecurity Performance Summary

Overseas Private Investment Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	At Risk	Consistently Implemented
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	2	2
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	7	8	9
Web	1	1	0
Other	1	3	2
Multiple Attack Vectors	0	0	0
Total	9	14	13

CIO Self-Assessment

While OPIC does not have High Value Assets (HVA), the Agency has determined that the greatest cybersecurity risks to the Agency's information systems are unauthorized access to Agency resources, unauthorized modification of the Agency's data and system configurations, and lack of availability of our payment system (OPIC's mission-essential function). To mitigate the risk of unauthorized access, OPIC maintains multifactor authentication (MFA) to both on-site and remote network access; performs periodic accounts reviews; and trains users to identify malicious emails designed to obtain network credentials.

OPIC's past assessments identified multiple known security vulnerabilities in endpoints and servers. To address these, OPIC is working to issue updated and hardened end points and servers during the first half of FY19. To mitigate the risk of unauthorized changes, OPIC is implementing the use of standard configurations with frequent scans to detect deviations.

Additionally, past audits have highlighted our lack of visibility to detect unauthorized hardware and software. As a result, OPIC is mitigating this weakness by participating in DHS' CDM initiative to implement tools and processes that will automatically detect new hardware and software in the enterprise.

To address the risk of lack of availability, OPIC has moved its financial systems to the Cloud, which provides higher availability due to its distributed and redundant architecture. OPIC has also established an offsite processing location to ensure continuity of access to the Agency's data.

OPIC's past assessments have determined the need to perform disaster recovery tests to ensure that redundancy measures are operating as expected. OPIC will plan and perform these tests in FY19.

Independent Assessment

The information security program of the Overseas Private Investment Corporation was evaluated as effective. OPIC's information security program was evaluated as part of the FY 2018 FISMA Audit. This audit included an evaluation of two OPIC-managed internal systems and four external systems. The FY 2018 audit noted that 65 of 72 selected NIST SP 800-53, Revision 4, security controls were properly implemented. This led to the determination of OPIC having an overall effective information security program. There were seven recommendations made to help OPIC improve their information security program. The recommendations can be found in the FY 2018 FISMA Audit report.

FY 2018 Annual Cybersecurity Performance Summary

Peace Corps

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	At Risk	Ad Hoc
Respond	At Risk	Defined
Recover		Ad Hoc
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	1	10	19
Loss or Theft of Equipment	0	1	1
Web	1	0	0
Other	4	1	5
Multiple Attack Vectors	1	0	0
Total	7	12	25

CIO Self-Assessment

In FY 2018, the agency began drafting an enterprise risk management program to create a firm foundation for its risk management responsibilities. In particular, new policy has been drafted, along with a Risk Management Committee charter and training material. Passage and implementation of the ERM program is expected in FY19. FY18 saw many policy, process and technical advances in the following areas:

- Revamped IT Security policy & processes
- Improved perimeter security (centralized and automated)
- Improved SEIM (improved to 100% visibility)
- CDM Phase 1 implementation underway (Will complete in FY19.)
- EINSTEIN 3a implemented (DNS only. Email component and TIC installation in FY19)
- BOD 18-01 implementation (Will complete in Q2 FY19; Peace Corps overseas Posts present complication few agencies have to mitigate.)

Independent Assessment

The information security program of the Peace Corps was evaluated as not effective. The independent assessment identified issues relating to the people, processes, technology, and culture aspects across all the Cybersecurity Framework Function areas. Moving forward, to advance and fully develop the information security program, involvement from all levels of the Peace Corps leadership is needed.

FY 2018 Annual Cybersecurity Performance Summary

Pension Benefit Guaranty Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	3	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	2	1	1
Loss or Theft of Equipment	27	0	0
Web	15	1	0
Other	4	2	0
Multiple Attack Vectors	0	0	0
Total	51	6	1

CIO Self-Assessment

The Pension Benefit Guaranty Corporation (PBGC) has identified its General Support System and 2 other major applications as HVAs. Potential risk factors to the agency include:

- Aging and outdated technology is constantly undergoing modernization.
- Data loss prevention, release or misuse controlled unclassified information including PII.
- Oversight of HVAs to include system's network segmentation from other systems and applications and the inability to encrypt data at rest for all Federal information.
- Inability to detect and prevent insider threats.
- Lack of an enterprise-wide IT supply chain management plan.
- Persistent system control deficiencies related to access and configuration management.

PBGC manages its risks by developing risk mitigation plans, creating Plans of Action and Milestones, implementing mitigation plans, and accepting risks where operational constraints exist. PBGC also employs programmatic strategies and approaches that ensure PBGC systems are compliant with the Corporation's Information Security Program and applicable laws and regulations. PBGC has established an IT RMF process to align with the NIST RMF.

The Corporation is maturing its enterprise risk management practices and improving risk-based prioritization of its resources for the replacement of IT Infrastructure components that have reached or are reaching end-of-service-life.

The Office of Information Technology (OIT) periodically briefs executives from each business unit about cybersecurity risks impacting their program. The CIO sponsors the PBGC Cybersecurity and Privacy Council comprised of Federal Information System Security Managers from the Corporation's business units with the goal of sharing information and making recommendations pertaining to cybersecurity and privacy.

Independent Assessment

The information security program of the Pension Benefit Guaranty Corporation was evaluated as not effective. The Pension Benefit Guaranty Corporation OIG contracted with an independent public accounting firm to perform the independent evaluation and review of the PBGC's information and technology security program as required by FISMA. Under OIG oversight, the review assessed the maturity of PBGC's information technology security program against FISMA reporting metrics.

In FY 2018, improvements to PBGC's incident response raised the maturity of that domain to managed and measurable; however, PBGC's overall information technology security program was not effective. The Corporation implemented many of its policies, procedures, and strategies but still needed to establish and incorporate quantitative and qualitative measures for many of the functional domains to be effective.

Recommendations for weaknesses as identified in risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring can be found in our FY 2018 Federal Information Security Modernization Act Independent Evaluation Report.

FY 2018 Annual Cybersecurity Performance Summary

Postal Regulatory Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

During this past year, the Commission has taken several steps to improve the overall security and performance of our systems and IT infrastructure. With new security threats continually emerging, we have established security practices and policies to better protect sensitive information and to educate employees about the importance of safeguarding the Commission's IT infrastructure, applications, and data.

The Commission conducted an annual Phishing exercise, trained our staff in cybersecurity awareness, and tested our Incident Response plan, Disaster Recovery plan, and Business Continuity Plan. The Commission continued to make cost effective improvements to our IT infrastructure by upgrading to a new, more secure wireless network and by implementing network segmentation and zoning, separating mission system servers to isolate them from all other network devices. By doing so, this follows security best practices and increases FISMA compliance.

The Commission completed the implementation of the DHS CDM program task group F. The Commission was the first small agency to fully implement CDM and report our security posture to the Federal dashboard. CDM's toolset has greatly improved identification of all hardware and software assets, identifies and prioritizes our risks and remediation efforts, and maintains compliance with OMB and other directives. The implementation of CDM, Einstein 3A, and Managed Trusted Internet Protocol Service greatly improved the Commission's cybersecurity posture providing us with the ability to identify incoming threats and mitigate those risks in near real time.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Postal Regulatory Commission was not performed for FY 2018, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Postal Regulatory Commission will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

Presidio Trust

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	At Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

In FY 2018, the Presidio Trust has advanced the security program in the areas of security staffing, security program funding, foundational elements of the security program and prevention of email-based attacks. The Presidio Trust has created and staffed a dedicated position to lead the security program, as of August 2018. Based on an external security assessment in late FY2017, the Presidio Trust has funded a FISMA project to advance the security program in 6 major areas of focus. These six areas are:

1) data identification, data classification, systems inventory and network segregation,
2) business continuity,
3) vulnerability management,
4) log aggregation and analysis,
5) security policies and procedures and
6) security training

Based on recent attack vectors, the Presidio Trust has implemented improved email configurations to prevent phishing, spear phishing and ransomware attacks.

Independent Assessment

Although an independent evaluation of the status of the Presidio Trust's IT cybersecurity program was completed in Q4 of FY 2017, an independent evaluation was not performed for FY 2018, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The Presidio Trust will explore contracting with an independent assessor annually starting in FY 2019 or in the subsequent initial years of the Information Security Program as determined by the implementation progress of the Program, the anticipated benefit of independent assessment and prioritization of necessary security work for the Program.

FY 2018 Annual Cybersecurity Performance Summary

Privacy and Civil Liberties Oversight Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Managed and Measurable
Detect	At Risk	Consistently Implemented
Respond	High Risk	Consistently Implemented
Recover		Managed and Measurable
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

Cybersecurity risks to the Privacy and Civil Liberties Oversight Board's (PCLOB) information assets include maintaining the availability and integrity of agency and partner data, which enables the Board's oversight and advisory functions and facilitates coordination with key stakeholders. Fortifying capabilities for privacy protected information throughout the enterprise is also an important driver in the agency's cybersecurity program.

As the agency develops and matures, elimination of impediments to timely, agile, and effective procurement processes are a key priority to ensure all legal, security, and contractual requirements are addressed to meet the organizations cybersecurity objectives. Another substantial cybersecurity risk facing the organization is an understrength IT workforce resulting in cascading impacts to the ability of the OCIO to further develop the security architecture while preserving security baselines, and to cultivate the knowledge and skills to achieve cybersecurity goals. This issue is exacerbated due to the agency's office relocation in the spring of 2018, which required significant IT resources for planning, engineering, and execution. The PCLOB took steps to addresses IT staff shortages by hiring an additional staff member. However, the staffing process did not did not complete until the end of Q4FY18.

Similar to many federal agencies, the PCLOB faces threats posed by Advanced Persistent Threats (APT) cyber criminals, and malicious insiders and must have the capabilities to quickly identify, contain, and respond to cybersecurity incidents. The PCLOB has been proactive implementing the DHS CDM Tools along with complementary defensive components.

Independent Assessment

The information security program of the Privacy and Civil Liberties Oversight Board was evaluated as effective. The PCLOB does not have an internal IG and has contracted with an independent auditor to conduct the FISMA IG Assessment. The PCLOB conducted its first independent audit in FY 2018. The results of the audit identified areas for improvement in the PCLOB security controls but noted the type and degree of deficiencies were expected for the first FISMA audit.

The PCLOB is proactive in remediating all identified deficiencies and strengthening existing security controls. The PLCOB also commissioned an independent vulnerability assessment of its IT infrastructure to gauge the effectiveness of its information security program. The resulting report stated that information systems exhibits "a better than average external and internal vulnerability profile" indicating effective implementation FISMA security controls.

The PCLOB has implemented MTIPS and CDM program and continues to steadily increase their security posture across all cybersecurity CAP goal targets.

FY 2018 Annual Cybersecurity Performance Summary

Railroad Retirement Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	15	5	0
External/Removable Media	1	0	0
Impersonation	1	NA	0
Improper Usage	18	20	23
Loss or Theft of Equipment	27	25	24
Web	0	2	0
Other	6	13	4
Multiple Attack Vectors	1	0	0
Total	69	65	51

CIO Self-Assessment

With the agency's planned development of a replacement distributed systems environment for the legacy systems architecture, information security risks will increase, and it will be critical for the Railroad Retirement Board (RRB) to implement an updated risk assessment for the new replacement system.

The RRB also recognizes that its cybersecurity program is still in need of improvement and acknowledges the cybersecurity risks identified in the five domains in the recent FY 2018 FISMA audit conducted by the RRB's OIG. Our goal is to remediate those cybersecurity risks as soon as possible.

The RRB must protect the PII of its annuitants and provide reliable access so they can claim their benefits. The RRB has a dedicated risk management team to monitor the network for intrusions, to make sure PII does not leave the network and to make security based decisions about the software and hardware allowed on the network.

The RRB has implemented a change control process and updated the Change Control Policy to ensure the RRB meets configuration management challenges. Included in the change control process is the requirement to submit a change request for any changes to the RRB information systems baseline configuration.

The RRB has performed an initial review of our HVAs and senior management is planning to perform a second review with stakeholders to identify all of the HVAs.

Independent Assessment

The information security program of the Railroad Retirement Board was evaluated as not effective. To assess how the Railroad Retirement Board (RRB) established and implemented its agency-wide Information Security Program and practices, as required by FISMA, an independent assessor performed detailed testing of RRB's Agency Enterprise General Information System (AEGIS), Benefit Payment Operations (BPO), Financial Management Integrated System (FMIS), and Financial Interchange (FI) systems and applications for compliance with selected controls from NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations.

FY 2018 Annual Cybersecurity Performance Summary

Securities and Exchange Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	0
E-mail	15	336	339
External/Removable Media	1	0	0
Impersonation	0	NA	0
Improper Usage	2	48	100
Loss or Theft of Equipment	0	2	1
Web	11	65	36
Other	14	63	74
Multiple Attack Vectors	0	12	2
Total	43	527	552

CIO Self-Assessment

The SEC completed a number of initiatives in FY18 to improve its cybersecurity posture. The last outstanding FY 2017 CAP goal was achieved. Full compliance with OMB M-15-13 and DHS (BOD) 18-01 were also achieved. The SEC made progress toward implementing the CSF by benchmarking the EDGAR system against CSF functions. The results were used to assess control maturity based on NIST security controls and FISMA Metrics. The SEC plans to continue CSF benchmarking activities for other HVAs.

The SEC aggressively worked to remediate audit recommendations. Overall, thirty-nine recommendations from the OIG and GAO were closed.

The SEC enhanced its cybersecurity training by delivering in-person privacy and security training to more than 1000 staff at six regional offices. Annual mandatory security and privacy training was improved by integrating the IT Rules of Behavior (ROB) into the SEC's learning management system, resulting in more efficient tracking of compliance by requiring staff to review and acknowledge the ROB annually. Greater than 99% compliance with annual privacy and security training requirements was achieved in FY18. Staff not meeting requirements were restricted from accessing SEC systems.

The SEC took steps to enhance capabilities to detect vulnerabilities and prevent attacks. A Working Group was established to enhance data protection and response capabilities. The SEC added staff, acquired outside support services, and utilized DHS cybersecurity resources. Einstein E3A was implemented to protect against malicious email, and progress was made to implement CDM. Multiple security assessments were conducted, including an independent pen-test and code review of the EDGAR system, and a DHS-led RVA Assessment of multiple SEC systems. SEC engaged with the DHS Hunt & Incident Response Team to search for indicators of malicious activity, and underwent a DHS "FIRE" Assessment of its cyber-incident-response capabilities.

Independent Assessment

The information security program of the U.S. Securities and Exchange Commission (SEC) was evaluated as not effective. The SEC made progress in enhancing information security policies and procedures to address security risks at the organizational and information system levels, strengthening authentication mechanisms, reducing the number of critical vulnerabilities, enhancing its security awareness and training processes, and continuing its efforts to enhance its continuous monitoring program. However, the SEC continues to face challenges with implementing a comprehensive risk management strategy, improving hardware and software asset management, enhancing its configuration management activities, improving the timeliness of security patch deployments, and re-establishing an alternate data center to recover mission-critical applications.

The SEC also has opportunities to improve the effectiveness of its vulnerability scanning activities, data protection and privacy activities, security training program, continuous monitoring strategy, and incident response capabilities. As a result, we determined that the SEC's information security program did not meet the definition of "effective."

FY 2018 Annual Cybersecurity Performance Summary

Selective Service System

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	21	59	0
Multiple Attack Vectors	0	0	0
Total	21	60	0

CIO Self-Assessment

DHS assessment of Selective Service System's (SSS) HVA concluded that additional controls will need to be implemented to enhance our current HVA infrastructure. Other risk includes aging infrastructure (equipment), and minimal manning in key positions. These items have been vetted with OMB, and are being addressed in FY19 budget.

Independent Assessment

The information security program of the Selective Service System was evaluated as effective. SSS's IT security program is rated overall at Managed and Measurable, which is considered to be an effective level of security at the domain, function, and overall program level. SSS had developed an agency-wide IT security program based upon assessed risk, and the security program provided reasonable assurance that the agency's information and information systems are appropriately protected.

FY 2018 Annual Cybersecurity Performance Summary

Small Business Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	1
E-mail	52	1	135
External/Removable Media	0	0	0
Impersonation	1	NA	0
Improper Usage	5	6	45
Loss or Theft of Equipment	19	39	16
Web	83	14	19
Other	58	80	128
Multiple Attack Vectors	5	3	0
Total	223	144	344

CIO Self-Assessment

During the past year, the SBA enhanced its deployment of IT controls and implemented the key components of the FITARA. The SBA made significant improvements in several areas of the Cybersecurity CAP Goal criteria, building a structured and resilient Cybersecurity program with notable advances in the areas of access controls, incident response, configuration and patch management, continuous monitoring, and data loss prevention. In addition, the SBA established enterprise capabilities in key areas such as penetration testing, cyber threat intelligence, cloud security, and end-point protection.

Independent Assessment

The information security program of the Small Business Administration was evaluated as not effective. Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, the OIG evaluated the design, implementation, and operating effectiveness of SBA's information security policies, procedures, and practices. The OIG determined that SBA has established and maintained its information security program and practices for the eight FISMA metric domains. However, the program was not fully effective as reflected deficiencies that we identified within all eight metric domains. We made new recommendations in these eight domains, and while SBA has worked to implement recommendations from previous FISMA reports, challenges remain in implementing an effective IT security program.

FY 2018 Annual Cybersecurity Performance Summary

Smithsonian Institution

Framework	CIO Rating	IG Rating
Identify	NA	Defined
Protect	NA	Consistently Implemented
Detect	NA	Defined
Respond	NA	Defined
Recover		Defined
Overall	High Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	7	3	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	2	2	4
Loss or Theft of Equipment	8	3	0
Web	7	6	2
Other	8	10	9
Multiple Attack Vectors	4	0	0
Total	36	24	15

CIO Self-Assessment

The Smithsonian Institution did not submit a self-assessment of their information security program and did not receive a risk management rating.

Independent Assessment

The information security program of the Smithsonian Institution was evaluated as not effective. An independent assessor selected two moderate impact Smithsonian Institution systems, SINET and Identity Management System (IDMS) to perform detailed testing for the FY 2018 FISMA audit.

The independent assessor also selected five moderate impact Smithsonian Institution systems, Personnel Security Case Management System (PSCMS), Security Management System (SMS), Human Resource Management System (ERP HRMS), EPMX, and Tessitura to perform additional testing for the protect and respond functions of the FY 2018 FISMA audit.

Based on our discussions with Smithsonian Institution personnel and inspection of the supporting documentation, the Smithsonian Institution has developed strategies and plans for most FISMA domains.

FY 2018 Annual Cybersecurity Performance Summary

Social Security Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	69	81	66
E-mail	26	112	67
External/Removable Media	1	5	0
Impersonation	3	NA	2
Improper Usage	196	1,059	1,547
Loss or Theft of Equipment	43	79	38
Web	40	349	501
Other	1,221	1,236	1,147
Multiple Attack Vectors	27	23	1
Total	1,626	2,944	3,369

CIO Self-Assessment

The Social Security Administration's (SSA) mission requires it to collect PII for over 325 million Americans. This information is vital to performing the agency's essential functions but makes its network, systems, and databases a rich target for adversaries.

As part of our FY 2017 Cybersecurity Risk Assessment report, we identified (1) the risk of a breach leading to a major loss of citizen data, (2) obtaining the skills needed to maintain aging systems, and (3) locally-developed applications as significant cyber risks. In FY2018, we made significant progress toward mitigating these risks. We continue to implement our agency IT Modernization plan to deploy our applications to our open systems architecture and retire legacy code. In accordance with the FCWAA, we coded our cyber and IT positions and identified areas of critical need. In FY2019, we are developing strategies to address critical cyber and IT skills gaps. In FY2018, we launched an initiative to consolidate our regional hosting environments into our primary agency data centers.

In the Identify area of the NIST framework: we increased our use of the cloud; expanded our supply chain risk analysis; and implemented stronger software and hardware asset management capabilities.

In the Protect area: we implemented DHS' trustworthy email and internet safeguard requirements; performed multiple risk and vulnerability assessments on our high value assets; implemented strong multi-factor authentication for our public facing citizen portal; implemented a strong privileged access management solution which issues temporary credentials for privileged functions; established sanctions to enforce mandatory awareness training; and implemented a new function to easily report suspected phishing attacks.

In the Detect area: we enhanced our intrusion detection and data loss prevention capabilities.

In the Recover area: we conducted multiple table top incident response exercises; and implemented new reporting procedures in response to US-CERT guidelines.

Independent Assessment

The information security program of the Social Security Administration was evaluated as not effective. Although SSA established an Agency-wide information security program and practices, the independent public accounting (IPA) firm contracted to perform the FISMA audit identified a number of deficiencies related to Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems.

FY 2018 Annual Cybersecurity Performance Summary

Surface Transportation Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Surface Transportation Board (STB) has worked hard to improve its information security program and remains committed to exceeding the bar set by the CIO FISMA Metrics. The STB continues to make steady improvements to mitigate and manage information security risk. At the organizational level, the STB has developed risk-related policies, procedures, and established the Risk Management Committee, which addresses risk at the organizational level. The STB has taken steps to protect organization information systems by implementing technical controls that block unauthorized endpoints from connecting to the Board's networks; enforce PIV authentication for general users and privileged user; and reduce the risk of external network connections for STB personnel.

The STB has also implemented a process of vulnerability detection and mitigation that decreases the information system attack surface of the STB. Finally, the STB has standardized its incident response procedures to comply with DHS US-CERT incident response best practices and guidance. Because of these efforts, the STB is able to meet or exceed the established CAP Goals for FY 2018.

Independent Assessment

The information security program of the Surface Transportation Board was evaluated as not effective. The STB has not fully developed strategies and plans for most FISMA domains. In addition, Surface Transportation Board has not fully defined information security related policies and procedures for the in-scope systems. Hence, the Board remains in an Ad Hoc level of maturity.

FY 2018 Annual Cybersecurity Performance Summary

Tennessee Valley Authority

Framework	CIO Rating	IG Rating
Identify	At Risk	Managed and Measurable
Protect	At Risk	Managed and Measurable
Detect	At Risk	Defined
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	7	0	1
External/Removable Media	3	1	0
Impersonation	0	NA	1
Improper Usage	22	13	7
Loss or Theft of Equipment	11	9	17
Web	3	7	0
Other	5	5	2
Multiple Attack Vectors	0	0	0
Total	51	35	28

CIO Self-Assessment

The Tennessee Valley Authority (TVA) works continually to identify and mitigate the Agency's cybersecurity risks. In FY 2018, the highest risks to TVA, its assets, and functions were unauthorized network connections and vulnerable software. To mitigate these, throughout FY 2018, TVA initiated and partially completed the implementation of network access control capabilities. This initiative was completed on TVA's large corporate facilities in FY 2018 and is planned to be completed throughout the agency in the out years. To mitigate the risk of insecure software, TVA Cybersecurity implemented ongoing active and passive scanning capabilities on its corporate network during FY 2018. This effort allowed TVA to better enumerate vulnerable hosts and manage remediation. It also allowed TVA to bring visibility to, and track risk to, its high value assets and ensure that those are being managed on an ongoing basis. During FY 2019, TVA will enhance processes around maintaining its patching program on an ongoing basis to further reduce the risk of insecure network assets.

TVA also identified the increasing use of cloud services as a risk and began implementation of a CASB solution to monitor TVA's information in the cloud. Technical testing and implementation will continue in FY 2019 and conclude in the out years. Finally, TVA has implemented user behavior analytics, and has established an insider threat working group comprised of TVA Police, TVA Cybersecurity, Human Resources, General Counsel, and TVA's Privacy Office to mitigate the risk associated with insider threat. This working group assesses behavioral and technical indicators to reduce the risk of intentional and unintentional insider threats.

Independent Assessment

Based on the analysis of the metrics and associated maturity levels defined by FISMA, the auditors found TVA's information security program was operating in an effective manner. In addition, analysis of the Detect metrics found TVA had developed an information security continuous monitoring (ISCM) strategy as part of its situational awareness program, and was in the process of implementing policies, processes, and tools in support of this strategy. However, TVA has not completed the development of policies and processes or the deployment of tools for the specific requirements within the ISCM strategy. FISMA requires each agency's IG to conduct an annual independent evaluation to determine the effectiveness of the information security program and practice of its respective agency. The audit objective was to evaluate TVA's information security program and agency practices for ensuring compliance with FISMA and applicable standards, including guidelines issued by OMB and NIST.

FY 2018 Annual Cybersecurity Performance Summary

United States AbilityOne Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	At Risk	Ad Hoc
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

AbilityOne Commission systems were assessed November 2017 by an independent assessor that identified 26 action item as part of its assessment. In 2018, the Committee closed 23 items and efforts are underway to close the remaining 3 POA&M items. The Commission currently has no identified HVAs in its infrastructure.

Independent Assessment

The information security program of the United States AbilityOne Commission was evaluated as effective. The Commission made progress with respect to the development of procedures and continued implementation of technology activities. The IT leadership focus on formalized and documented policies, and the emphasis to consistently implement IT requirements for its operational environment. Furthermore, the Commission strives to make additional improvements in the areas of vulnerability scanning, incident response plan, and information security policies for continued overall assessment of the agency's information security program and practices.

FY 2018 Annual Cybersecurity Performance Summary

United States Access Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	NA
Protect	At Risk	NA
Detect	Managing Risk	NA
Respond	Managing Risk	NA
Recover		NA
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

To strengthen our information security policies and processes, we have an IT support system contract to administer security controls, standard operating procedures, and a Program of Actions and Milestones specified in our ATO. Our current IT support system contract supplies the Access Board with the same security software tools that are available under the CDM program, however, the Board anticipates transitioning the Access Board's software tools over to the CDM program. This year the Access Board has mitigated a significant number of our Cybersecurity risks due to the implementation of the NIST 800-53 security controls. The Board has made significant improvements in our CAP Goals and information security practices through our IT support system contract. The Access Board's security policies and processes must be improved in the areas of system authorization and credentialing. However, the Board believes that our participation in the CDM initiative will substantially improve our Cybersecurity Risk Framework. The Board is working with the GSA to transition from GSA WITS3 to GSA EIS and plan to implement our MTIPS/TIC requirement however, our anticipation implementation date has moved due to the GSA EIS incomplete transition process.

The Board will continue to improve our cybersecurity posture and information security baseline. However, the Board is currently unable to meet all Cybersecurity and FISMA requirements due to the lack of available funds and lack of staffing resources to support these Cybersecurity and Critical Network Infrastructure initiatives.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the United States Access Board was not performed for FY 2018, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The United States Access Board will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

United States Agency for International Development (USAID)

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	1	0
E-mail	8	7	2
External/Removable Media	0	0	0
Impersonation	0	NA	2
Improper Usage	2	10	15
Loss or Theft of Equipment	8	30	9
Web	20	21	8
Other	93	123	20
Multiple Attack Vectors	0	0	0
Total	131	192	56

CIO Self-Assessment

USAID has identified three high value systems that support the Agency's mission essential functions. These three systems contain sensitive financial data, PII, and sensitive foreign affairs information. It will have a significant operational impact if these HVAs are compromised.

In addition to the DHS' HVA Risk and Vulnerability assessment conducted during May 2017, USAID CIO conducts regular internal vulnerability assessments and independent penetration tests. USAID has remediated all of the security weaknesses identified by the DHS assessment team and is re-validating the security controls implemented with DHS currently.

Lastly, these three systems were part of the USAID's annual COOP exercise where the Agency's senior leadership participated in a tabletop exercise with a scenario of cyber attacks on the HVAs.

Independent Assessment

The information security program of the United States Agency for International Development was evaluated as effective. USAID's information security program was evaluated as part of the FY 2018 FISMA Audit. This audit included an evaluation of 6 out of 47 FISMA reportable systems at USAID. The FY 2018 FISMA Audit noted 120 of 135 selected NIST 800-53, Revision 4 security controls were properly implemented. This led to the determination of USAID having an overall effective information security program. There were a few recommendations made to help USAID improve their information security program. These recommendations can be found in the FY 2018 FISMA Audit report.

FY 2018 Annual Cybersecurity Performance Summary

United States Interagency Council on Homelessness

Framework	CIO Rating	IG Rating
Identify	At Risk	NA
Protect	At Risk	NA
Detect	At Risk	NA
Respond	Managing Risk	NA
Recover		NA
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

Per NIST SP 800-60, United States Interagency Council on Homelessness' (USICH) sole information system is categorized as Low Impact. For FY 2018, USICH has continued to update its system security plan, as it is a living document that will be updated periodically to incorporate new and/or modified security controls. The plan will continue to be revised as the changes occur to the system, the data or the technical environment in which the system operates.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the United States Interagency Council on Homelessness was not performed for FY 2018, and the IG assessment section is marked "Not Applicable (NA)". Per FISMA, Sec. 3555(b)(2), where agencies do not have 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. The United States Interagency Council on Homelessness will explore contracting with an independent assessor in FY 2019.

FY 2018 Annual Cybersecurity Performance Summary

United States Trade and Development Agency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY16	FY17	FY18
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	0	0	2

CIO Self-Assessment

U.S. Trade and Development Agency (USTDA) has worked very hard over the last fiscal year to continuously improve and enhance the security of our information services. USTDA improved the number of our Plan of Action and Milestone closures by 147%, with 17 POAM items closed in FY2017, with 42 POAM items closed in FY2018.

USTDA improved vulnerability remediation percentage from 77% in FY 2017, to 98% in FY 2018, which amounts to an improvement of 21 percentage points. USTDA has increased the number of our IT policies mapped to NIST 800-53 standards from four in FY 2017, to eight in FY 2018. Further, USTDA improved from 12% of PCs running Windows 10 DoD DISA STIG standard configured systems in FY 2017, to 100% of our PCs running Windows 10 standard configuration in FY 2018. USTDA met all ten CAP goal requirements in FY 2018, exceeding the requirements for six of the goals.

Independent Assessment

The information security program of the U.S. Trade and Development Agency was evaluated as effective. This is an independent audit determined USTDA effective by our audit company. The USTDA security program continues to be incorporated into its annual performance and security plans in accordance with the law, providing reasonable assurance and safeguards to maintain integrity, and competence.

FY 2018 Annual Cybersecurity Performance Summary

Vietnam Education Foundation

Framework	CIO Rating	IG Rating
Identify	High Risk	Defined
Protect	At Risk	Consistently Implemented
Detect	High Risk	Ad Hoc
Respond	At Risk	Defined
Recover		Defined
Overall	High Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	0	0	0

CIO Self-Assessment

The Vietnam Education Foundation (VEF) has implemented appropriate measures to protect its information systems against cybersecurity attacks while making preparations for its permanent closure in 2018.

Independent Assessment

The information security program of the Vietnam Education Foundation was evaluated as effective. The VEF has implemented appropriate measures to protect the agency's information security program. As a micro-agency of 4 employees which will sunset in 2018, the VEF will continue to work toward compliance but lack the resources to implement some requirements.

Appendix I: 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
DHS – Department of Homeland Security
ERM – Enterprise Risk Management
FedRAMP – Federal Risk and Authorization Management Program
FY – Fiscal Year
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
RMF – Risk Management Framework
RVA – Risk and Vulnerability Assessment
SAOP – Senior Agency Official for Privacy
SCAP – Security Content Automation Protocol
SWAM – Software Asset Management
TIC – Trusted Internet Connection
US-CERT – United States Computer Emergency Readiness Team