



# Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2019

*The Office of Management and Budget (OMB) is publishing this report in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, § 3553, 44 U.S.C. § 3553. This report also incorporates OMB's analysis of agency application of the intrusion detection and prevention capabilities, as required by Section 226(c)(1)B) of the Cybersecurity Act of 2015, Pub. L. No. 114-113. OMB obtained information from the Department of Homeland Security (DHS), Chief Information Officers (CIOs) and Inspectors General (IGs) from across the Executive Branch to compile this report. This report primarily includes Fiscal Year 2019 data reported by agencies to OMB and DHS on or before October 31, 2019.*



# Table of Contents

- Executive Summary: The State of Federal Cybersecurity..... 5
  - A. Federal Cybersecurity Roles and Responsibilities..... 6
- Section I: Federal Cybersecurity Activities..... 9
  - A. Increasing Cybersecurity Threat Awareness..... 9
  - B. Standardizing Cybersecurity and IT Capabilities..... 11
  - C. Maturing Security Operations Centers (SOCs) ..... 15
  - D. Driving Agency Accountability..... 15
- Section II: Senior Agency Official for Privacy (SAOP) Performance Measures..... 19
  - A. Senior Agency Officials for Privacy (SAOPs) and Privacy Programs..... 19
  - B. Personally Identifiable Information and Social Security numbers..... 20
  - C. Privacy and the Risk Management Framework ..... 22
  - D. Information Technology Systems and Investment ..... 25
  - E. Privacy Impact Assessments..... 25
  - F. Workforce Management..... 27
  - G. Breach Response and Privacy..... 29
- Section III: FY 2019 Agency Performance ..... 32
  - A. Introduction to Cybersecurity Performance Summaries ..... 32
  - B. FY 2019 Information Security Incidents ..... 36
  - C. Agency Cybersecurity Performance Summaries ..... 39
- Appendix I: Commonly Used Acronyms ..... 40

# Executive Summary:

## The State of Federal Cybersecurity

Cybersecurity threats facing the Federal Government and our Nation reinforce the need for strengthening the digital defense of the country's information technology (IT) environment. America's infrastructure, both public and private, continues to be a top target of malicious cyber actors intent on disrupting the geopolitical and socioeconomic stability and prosperity of the United States. This persistent threat is a constant reminder that effective cybersecurity is required by all organizations — public and private — to identify, prioritize, and manage cyber risks across their enterprise.

The [President's Management Agenda](#) (PMA) sets a clear goal to modernize the Federal Government's information systems. The path forward will continue to rely on the maturation of cybersecurity efforts across Federal agencies in order to reduce operational risk and provide secure services for the American public. In September 2018, the President released the [National Cyber Strategy](#), which outlined objectives for defending the homeland and promoting American prosperity by protecting public and private systems and information and 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 to enhance cybersecurity risk management across the Federal Government. Executive Order 13800 recognizes the importance of mission delivery, service quality and securing citizens' information even as malicious cyber actors seek to disrupt those services.

This report highlights that Fiscal Year (FY) 2019 has begun to show the cybersecurity improvements due to the decisive actions the Administration has taken to address high risk areas for the Federal Government. Updated policies around High Value Assets (HVAs), Trusted Internet Connections (TIC), and Identity Credential and Access Management (ICAM) have been coupled with Department of Homeland Security (DHS) programs and directives to empower agencies to mitigate risks across the Federal Government. We have efforts underway to further enhance cybersecurity in the areas of supply chain risk, Security Operations Center (SOC) maturation, and third party privacy risk. As progress continues, the executive and legislative branch must continue its collaboration to confirm there is sustained momentum for addressing these critical capability gaps.

Agencies reported 28,581 cybersecurity incidents in FY 2019, an 8% decrease over the 31,107 incidents that agencies reported in FY 2018. The decline in incidents is correlated with the continued maturation of agencies' information security programs. In FY 2019, a total of 72 agencies received an overall rating of "Managing Risk" in the annual cybersecurity Risk

Management Assessment (RMA) process (detailed in Section III of this report), up from 33 agencies in FY 2017 and 62 agencies in FY 2018. However, this decline in incidents reported in no way indicates a reduction in the cybersecurity threat posed to the Federal Government.

Accordingly, this report to Congress on the implementation of the [Federal Information Security Modernization Act of 2014](#) (FISMA) highlights government-wide programs and initiatives as well as agencies' progress to enhance Federal cybersecurity over the past year.

## A. Federal Cybersecurity Roles and Responsibilities

FISMA identifies the agency head as the responsible official for their respective organization's cybersecurity posture, and Executive Order 13800 reinforces this responsibility. Agencies are responsible for allocating the necessary people, processes, and technology to protect Federal data. Each agency head is responsible for delegating this authority to the Chief Information Officer (CIO), including the authority to designate a Senior Agency Information Security Officer or Chief Information Security Officer (CISO).

Enhancing Federal cybersecurity is a collective effort that requires participation from all personnel across the Federal enterprise. The following section provides a brief overview of 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 statutorily 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 leaders. 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), Cybersecurity and Infrastructure Security Agency (CISA):** CISA is the operational lead for government-wide Federal cybersecurity and

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

**General Services Administration (GSA):** GSA provides management and administrative support to the entire Federal Government, and establishes acquisition vehicles for agencies to purchase cybersecurity products and services. Additionally, GSA provides administrative assistance for the Chief Information Officers Council and Chief Information Security Officers Council. 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, develops standards and guidelines for Federal information systems, in coordination with OMB and other Federal agencies. Among other roles, NIST creates Federal Information Processing Standards (FIPS) and provides management, operational, and technical security guidelines on a broad range of topics, including intrusion detection, incident handling, supply chain risk management, and definition of strong authentication protocols. NIST develops, updates, and publishes a series of frameworks, including the [Framework for Improving Critical Infrastructure Cybersecurity](#) (NIST Cybersecurity Framework).

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

---

<sup>1</sup> 44 U.S.C. § 3553(h)(1)-(2)

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

## Section I: Federal Cybersecurity Activities

The President has made strengthening the Nation’s cybersecurity a priority from the outset of this Administration. Executive Order 13800 reinforces FISMA by holding agency heads accountable for managing cybersecurity risks to their enterprises<sup>2</sup> and requiring each agency to assess its cybersecurity risks and submit a plan to OMB detailing actions to implement the NIST Cybersecurity Framework.<sup>3</sup>

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](#), describes activities to modernize and safeguard high-risk 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 \(Risk Determination Report\)](#), 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 FY 2019, 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 2019 is organized in alignment with the actions from this report.

### A. Increasing Cybersecurity Threat Awareness

Numerous government and industry cybersecurity reports continue to highlight the persistent threat posed by malicious cyber actors. The sophistication of techniques operationalized by these groups combined with an expanded attack surface,<sup>4</sup> increases the

---

<sup>2</sup> 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.

<sup>3</sup> 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>

<sup>4</sup> The expansion of the attack surface is the result of the continued interconnection of networks, devices, and services managed within organizations

risk of compromise to information systems. Gathering, analyzing, and disseminating threat information is vital to effectively managing government cybersecurity risk. Efforts continue within the government to improve operationalizing threat information to better protect the Federal IT environment. To increase the awareness of cyber threats, OMB and DHS continue to integrate efforts improve the quality, effectiveness, and scale of the government’s threat-related programs.

### National Cybersecurity Protection System

The National Cybersecurity Protection System, of which the EINSTEIN system is a component, provides a suite of tools to enhance the boundary awareness and security of Federal agencies. The most recent of these capabilities is EINSTEIN 3 Accelerated (E3A), an integrated intrusion prevention, detection, and analysis system that builds on the passive detection capabilities of EINSTEIN 1 and EINSTEIN 2. The E3A program aggregates Federal civilian executive branch traffic enabling the deployment of new and advanced protections by DHS. As of September 30, 2019, DHS reports that, of 104 Federal civilian agencies, 76 (up from 70 in FY 2018) report implementing all three NCPS capabilities, including all 23 civilian CFO Act agencies.

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

<b>EINSTEIN Capability</b>	 <b>Complete</b>	 <b>In Progress</b>	 <b>Deferred<sup>5</sup></b>	 <b>Not Implemented</b>
<b>E1/E2</b>	76	0	0	28
CFO	23	0	0	0
Non-CFO	53	0	0	28
<b>E3A Email</b>	78	5	3	18
CFO	23	0	0	0
Non-CFO	55	5	3	18
<b>E3A DNS</b>	82	4	1	17
CFO	23	0	0	0
Non-CFO	59	4	1	17

<sup>5</sup> 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.

## B. Standardizing Cybersecurity and IT Capabilities

Agency risk assessments have demonstrated that a lack of standardization and insufficient access to common capabilities have hindered agencies' ability to mitigate vulnerabilities and other cybersecurity challenges. OMB continues to work to effectively adapt current security practices to a more modern technology landscape while increasing standardization across Federal Agencies. This includes efforts such as enhancing the HVA program, maturing government-wide ICAM, modernizing the TIC program, and integrating supply chain risk management into procurement activities.

### Continuous Diagnostics and Mitigation (CDM)

The Continuous Diagnostics and Mitigation (CDM) Program enhances the overall security posture of the Federal Government by providing Federal agencies with capabilities to monitor access (human and non-human), assets, and traffic of their networks in near real-time. This increased situational awareness allows agencies to manage cybersecurity vulnerabilities based on severity of risk. CDM program team collaborates with agencies to deploy commercial off-the-shelf tools on their networks. Object-level information is made available to the agencies through their CDM Agency Dashboard and is also summarized to the CDM Federal Dashboard for awareness and action at the federal level by OMB and CISA.

All 23 civilian CFO Act agencies currently report object-level data to their CDM Agency Dashboards and the CDM Federal Dashboard. The CDM Program Office has established a cloud based CDM Shared Services Platform which provides non-CFO Act agencies with access to their own dashboard. Thirty non-CFO Act agencies are reporting object-level data to the CDM Shared Service Platform and the CDM Federal Dashboard. In an effort to continue advancing capabilities for all agencies, the CDM Program Office, in partnership with GSA, has awarded the new CDM Dashboard Ecosystem contract that will provide better analytics, business intelligence, and data visualizations for civilian agencies and federal leadership. The CDM Dashboard Ecosystem will be deployed in FY 2020, and progress of agencies' implementation of CDM will be reflected in [DHS' FY 2020-2021 Agency Priority Goal, "Strengthen Federal Cybersecurity."](#)

### Vulnerability Disclosure Policy (VDP)

As Federal agencies continue to expand their digital footprints, cybersecurity risks to their information systems requires a secure channel for the public and researchers to report security issues in order to reduce the potential impact of identified security flaws. In response to the evolving challenge of identifying and managing vulnerabilities within Federal networks, OMB released a draft memorandum for public comment, with the final version of the guidance to be issued in 2020. The final guidance mandates a baseline of government-wide Coordinated Vulnerability Disclosure (CVD) requirements.

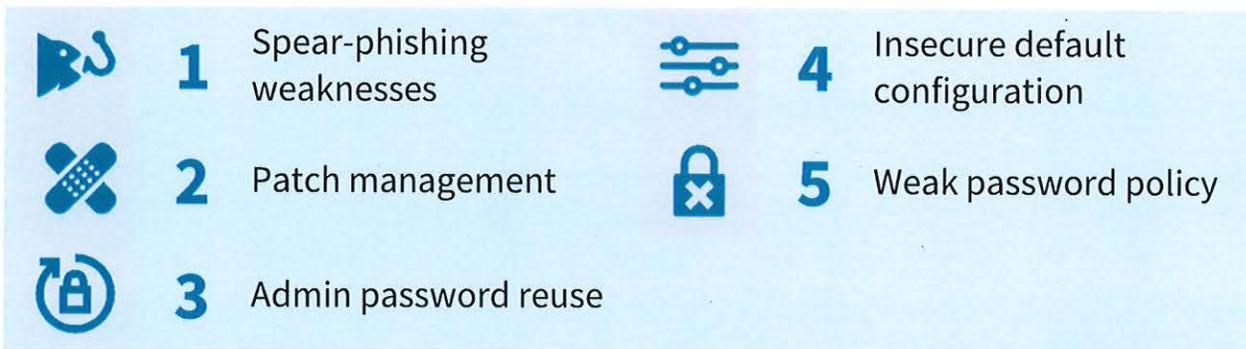
## High Value Assets (HVAs)

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

In order to build on the guidance provided in [OMB Memorandum M-19-03, \*Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program\*](#), OMB worked with DHS CISA to enable a data-driven and repeatable process for prioritizing HVA management activities and resources across the Federal government. This includes revising the data call for the [DHS BOD 18-02, Securing High Value Assets](#), in which agencies are required to review the Agency HVA list on a quarterly basis and provide updates and modifications to CISA.

In FY 2019, DHS conducted 71 HVA assessments (up from 61 assessments in FY 2018), resulting in 448 findings (up from 356 findings in FY 2018), consisting of 204 System Architecture Review findings and 244 Risk and Vulnerability Assessment (RVA) findings. These assessments revealed that the Federal Government continues to face challenges mitigating basic security vulnerabilities. The most common security deficiencies identified across the HVA landscape are identified in Figure 1. Progress of agencies’ ability to respond to HVA recommendations will be reflected in [DHS’ FY 2020-2021 Agency Priority Goal, “Strengthen Federal Cybersecurity.”](#)

**Figure 1 Top 5 RVA findings in FY 2019**



## Trusted Internet Connections (TIC)

The need to enhance the policies for network security across the Federal Government is another priority raised specifically in the [Report to the President on the Modernization of Federal IT](#), and is necessary to facilitate the adoption of modern technology solutions. Historically, network security has been accomplished by routing Federal internet traffic

through a limited number of access points where security measures were deployed. Changes to the way the Federal Government utilizes technology, particularly its increased use of cloud-based infrastructure, necessitated an update to the previous approach. To accomplish this, OMB worked in close collaboration with DHS, GSA, and a select set of agencies to initiate and oversee TIC modernization pilots. The pilots sought to deliver similar security benefits as the TIC program while allowing greater flexibility in delivering IT services. The results of the lessons learned from these pilots were used to the development of [OMB Memorandum M-19-26, Update to the Trusted Internet Connections \(TIC\) Initiative](#). The new memo:

- **Removes 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.
- **Ensures 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, with input from both industry and Federal agencies, for continuously updating the TIC initiative’s implementation guidance. This process facilitates ongoing piloting and approval of new and innovative methods to achieve TIC Initiative security objectives in the most effective and efficient manner.
- **Streamlines the Agency Implementation Processes** – The goal is to shift from burdensome, point-in-time, manual spot checks to a scalable, comprehensive, and continuous validation process.

In FY 2020, DHS in coordination with OMB and the CISO Council, is expected to explore additional pathways for TIC implantation via new TIC use cases. The TIC use case documentation will outline alternative security controls to maintain proper visibility of the Federal computing environment as agencies modernize their IT architectures.

### Supply Chain Risk Management (SCRM)

The National Cyber Strategy includes a priority action to improve Federal supply chain risk management. A critical component of this approach is the integration of supply chain risk management into each procurement of information and communications technology (ICT) goods or services. In December 2018, the President signed into law the SECURE Technology Act (Public Law 115-390), which provides a major step toward implementing the supply chain risk management requirements called for in the National Cyber Strategy. Under the SECURE Technology Act, departments and agencies are required to assess the risks to their ICT supply chains by establishing a SCRM program.<sup>6</sup>

---

<sup>6</sup> 41 USC 1326 (a) (1).

In FY 2019 OMB established the Federal Acquisition Security Council (FASC). The FASC is charged with developing criteria for federal SCRM programs, criteria for sharing relevant supply chain risk information, and protecting Federal IT by recommending the exclusion or removal of dangerous products.

### Identity, Credential, and Access Management (ICAM)

As the evolution of service delivery continues to trend towards digital channels, the importance of implementing security controls designed to effectively protect data and manage access continues to be a priority for the Federal Government.

Pursuant to recommendations outlined in the Report to the President on Federal IT Modernization OMB released [OMB Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management](#) on May 21, 2019, OMB M-19-17 shifts agency ICAM strategies and solutions from the obsolete Levels of Assurance (LOA) model to a risk management methodology, enabling agency resource decisions to be aligned to agency mission priorities. The guidance defines the following:

- Sets a foundation for agency implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, and any successive versions.
- Reinforces Homeland Security Presidential Directive 12 (HSPD-12) as the Government wide policy for the promulgation of standards-based, secure, and reliable forms of identification across the Federal Government enterprise, as outlined by Federal Processing Standard (FIPS) 201-2.
- Directs agencies to establish integrated, agency wide, ICAM offices, teams, or other governance structures to facilitate effective governance and enforcement of ICAM efforts leveraging an enterprise risk management approach.
- Promotes architectural design guidelines that encourages the use of commercially available products, drives the management of digital identity lifecycle of devices, and requires agencies to leverage privacy enhanced data-validation services for access to data.
- Drives acquisition compliance to HSPD-12, FIPS 201, OMB policy, NIST standards, for all ICAM contract activities, and requires the adoption and use of the CDM program.

These efforts are driven by a resurgence in public-private partnerships tackling key issues for agencies as they drive towards modern architectures. The improvements to ICAM will continue to drive unified methodologies, governance, and application of capabilities and services focused on improving public access protections to sensitive data and, the Federal Government's continued efforts to implement end-to-end security reducing threat exposure from criminal and state-sponsored actors.

## C. Maturing Security Operations Centers (SOCs)

As noted in the *Risk Determination Report*, Federal agencies often lack centralized visibility into their networks necessary to effectively detect data exfiltration attempts and rapidly respond to cybersecurity incidents. This gap stems from two operational issues. At smaller agencies, there are often insufficient number of fulltime employees with the requisite skills to operate a SOC effectively. At larger agencies, it is often also a result of numerous SOCs that do not effectively communicate with each other in a manner that supports rapid response. This fractured security landscape can be a significant impediment and contribute to diminished network visibility and inefficient and ineffective operations. As part of OMB's broader shared services effort outlined in [OMB Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government](#), DHS has been designated as a Quality Services Management Office (QSMO) for cybersecurity. DHS and OMB are working with agencies to develop a SOC as a service offering for streamlined detection, analysis, and response activities. This approach includes creating a standardized maturation assessment process and developing a structured centralized source for approved SOC capabilities.

## D. Driving Agency Accountability

While the priority placed on Federal cybersecurity has been clear, metric-based, proactive oversight is necessary to measure both the progress agencies make over time as well as hold agency leaders accountable when they fail to meet established targets. Pursuant to Executive Order 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

OMB regularly collects cybersecurity spending data as part of its budgeting and oversight role, and has aligned the spending categories of these data collections to capabilities in the NIST Cybersecurity Framework and FISMA performance metrics. The outcome of this alignment has led to a common vocabulary and taxonomy that agencies can use to make resourcing decisions that affect their operational and cybersecurity risk posture. OMB continues to refine these definitions and work with agencies to integrate best practices into agency strategic planning and risk management functions in concert with agency CIOs, CISOs, and CFOs.

A summary of cybersecurity spending for FY 2019 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.

**Table 2 FY 2019 Cybersecurity Spending**

<b>Agency</b>	<b>FY 2019 Spend (\$ Millions)</b>	<b>Agency</b>	<b>FY 2019 Spend (\$ Millions)</b>
Commerce	\$446.4	NASA	\$167.6
DHS	\$2,590.8	NRC	\$28.8
DOD	\$8,527.0	NSF	\$246.4
DOT	\$216.4	OPM	\$40.9
ED	\$119.0	SBA	\$16.3
Energy	\$578.4	SSA	\$204.0
EPA	\$42.1	State	\$381.5
GSA	\$72.6	Treasury	\$510.8
HHS	\$512.5	USAID	\$62.6
HUD	\$60.8	USDA	\$208.2
Interior	\$103.8	VA	\$491.7
Justice	\$837.2	Non-CFO Act	\$384.3
Labor	\$86.6		
		<b>Total</b>	<b>\$16,936.9</b>

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

Section 3553 of title 44, U.S. Code, authorizes DHS to develop and oversee the implementation of cybersecurity Binding Operational Directives (BODs) and Emergency Directives (EDs), which outline activities federal agencies are required to comply with. BODs address agency implementation of OMB policies, principles, standards, and guidelines. EDs address known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to agency information security.

CISA leads DHS efforts to develop, communicate, and manage actions and critical activities related to all directives, in close coordination with OMB. DHS issued one BOD and one ED in FY 2019:

- Emergency Directive 19-01: Mitigate DNS Infrastructure Tampering:** In coordination with government and industry partners, CISA was tracking a series of incidents involving Domain Name System (DNS) infrastructure tampering. CISA suspected that multiple executive branch agency domains were affected by the tampering campaign and has notified the agencies that maintain them. To address the significant and imminent risks to agency information and information systems presented by this activity, this Emergency Directive issued on January 22, 2019, required the following near-term actions to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains, and detect unauthorized certificates: 1) audit DNS records; 2) change DNS account passwords; 3) add multi-factor authentication to DNS accounts; and 4) monitor certificate transparency logs.
- Binding Operational Directive 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems:** As federal agencies continue to expand deployment of Internet-accessible systems, and operate interconnected and complex systems, it is critical for them to rapidly remediate vulnerabilities that compromise federal networks through exploitable, externally-facing systems. The federal government must continue to take deliberate steps to reduce the overall attack surface and minimize the risk of unauthorized access to federal information systems.

On May 21, 2015, Binding Operational Directive 15-01: Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies' Internet-Accessible Systems, established requirements for federal agencies to review and remediate critical vulnerabilities on Internet-facing systems identified by the National Cybersecurity and Communications Integration Center (NCCIC) within 30 days of issuance of their weekly Cyber Hygiene report. Since its issuance, the prior National Protection and Programs Directorate (NPPD) and the current CISA oversaw a substantial decrease in the number of critical vulnerabilities over 30 calendar-days, as well as significant improvements in how agency teams identified and responded to these vulnerabilities in a timely manner. By implementing specific remediation actions, continuous monitoring, and transparent reporting through CISA's Cyber Hygiene service, BOD 15-01 helped drive progress and enhance the federal government's security posture.

On April 29, 2019, CISA issued BOD 19-02, which supersedes BOD 15-01. BOD 19-02 ensures timely remediation of critical and high vulnerabilities identified through Cyber Hygiene scanning and requires federal agencies to complete the following actions: 1) Ensure access and verify scope for Cyber Hygiene scanning; and 2) Review and remediate critical and high vulnerabilities within 15 and 30 calendar days, respectively.

## Enhancing Cybersecurity Oversight

Consistent with other efforts to help agencies understand their cybersecurity risk profiles, OMB and DHS have continued to work with the CIO and 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 continued iteration on 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. In addition, the FY2021 Budget included additional categorization of resources aligned to the specific activities for Identify, Protect, Detect, Respond, and Recover.

## 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 information (PII) to carry out its missions and programs. In today’s digital world, effectively managing the risk to individuals associated with the Federal Government’s processing of their PII depends on Federal agencies maintaining robust privacy programs.

For FY 2019, all 24 CFO Act agencies and 57 non-CFO Act agencies reported SAOP FISMA performance measures to OMB.

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

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

Each Federal agency is required to develop, implement, document, maintain, and oversee an agency-wide privacy program that includes people, processes, and technologies. The agency’s SAOP leads the agency’s privacy program and is responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency’s mission. Among other things, where PII is involved, the agency’s privacy program plays a key role in information security, records management, strategic planning, budget and acquisition, contractors and third parties, workforce, training, incident response, and implementing the National Institute of Standards and Technology’s (NIST) Risk Management Framework (RMF).<sup>7</sup>

---

<sup>7</sup> 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**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The head of the agency has designated an SAOP. <sup>8</sup>	100%	98%
Among the agencies that have designated an SAOP: The SAOP has the necessary role and responsibilities to ensure compliance with applicable privacy requirements. <sup>9</sup>	100%	100%
The SAOP has the necessary role and responsibilities to develop and evaluate privacy policy. <sup>10</sup>	100%	100%
The SAOP has the necessary role and responsibilities to manage privacy risks consistent with the agency’s mission. <sup>11</sup>	100%	100%
The agency has developed and maintained a privacy program plan. <sup>12</sup>	100%	88%
Among the agencies that have developed and maintained privacy program plans, the agency identifies and plans for the resources needed to implement the agency’s privacy program. <sup>13</sup>	92%	94%

## **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.

<sup>8</sup> See OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).

<sup>9</sup> See *id.*

<sup>10</sup> See *id.*

<sup>11</sup> See *id.*

<sup>12</sup> Federal agencies are required to develop and maintain a privacy program plan that provides an overview of the agency’s privacy program, including a description of the 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).

<sup>13</sup> See *id.* at Appendix I § 4(b)(1).

## Table 4 Personally Identifiable Information Inventory

FY 2019 – SAOP FISMA Performance Measures	CFO	Non-CFO
The agency maintains an inventory of the agency’s information systems <sup>14</sup> that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. <sup>15</sup>	100%	91%

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. Therefore, 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 2019 – SAOP FISMA Performance Measures	CFO	Non-CFO
Among the agencies that collect, maintain, or use SSNs, the agency has an inventory of the agency’s collection and use of SSNs. <sup>16</sup>	96%	91%
Among the agencies with SSN and information systems inventories, the agency maintains its inventory of SSNs as part of the agency’s inventory of information systems.	96%	83%
The agency has developed and implemented a written policy to help ensure that any new collection or use of SSNs is necessary.	92%	74%

<sup>14</sup> The term “information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See 44 U.S.C. § 3502(8). The term “information resources” means information and related resources, such as personnel, equipment, funds, and information technology. See 44 U.S.C. § 3502(6). The term “Federal information system” means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 10(a)(23) (July 28, 2016).

<sup>15</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(a)(1)(a)(ii), 5(f)(1)(e) (July 28, 2016).

<sup>16</sup> Federal agencies are not required to have an inventory of collection and use of SSNs. However, agencies need to have a sufficient evidentiary basis to determine whether they have met the requirement to eliminate unnecessary collection and use of SSNs.

Among the agencies with such written policies: The agency's written policy provides specific criteria to use when determining whether the collection or use of SSNs is necessary.	95%	81%
The agency's written policy establishes a process to ensure that any collection or use of SSNs remains necessary over time.	91%	88%
If the agency has not successfully eliminated all unnecessary collections, maintenance, and uses of SSNs at the agency, the agency took steps during the reporting period to eliminate the unnecessary collection, maintenance, and use of SSNs. <sup>17</sup>	100%	94%

### C. Privacy and the Risk Management Framework

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

**Table 6 Privacy and the NIST Risk Management Framework**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency implemented a risk management framework to guide and inform the following: Categorization of Federal information and information systems that process PII. <sup>18</sup>	100%	94%
Selection, implementation, and assessment of privacy controls. <sup>19</sup>	100%	90%
Authorization of information systems and common controls. <sup>20</sup>	100%	92%

<sup>17</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, § 5(f)(1)(f) (July 28, 2016).

<sup>18</sup> See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 3(a), 3(b)(5) (July 28, 2016).

N/A responses are not included in the percentages.

<sup>19</sup> See *id.*

<sup>20</sup> See *id.*

Continuous monitoring of information systems that process PII. <sup>21</sup>	100%	77%
The agency designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls. <sup>22</sup>	88%	70%
The agency has developed and maintains a written privacy continuous monitoring strategy. <sup>23</sup>	83%	63%
The agency has established and maintains an agency-wide privacy continuous monitoring program. <sup>24</sup>	79%	58%

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.

<sup>21</sup> See *id.*

<sup>22</sup> See *id.* at Appendix I § 4(e)(5); see also *id.* at § 10(a)(14), (26), (66) and (86).

<sup>23</sup> The SAOP is required to develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix I § 4(d)(9), 4(e)(2) (July 28, 2016).

<sup>24</sup> The SAOP is required to establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and 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**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The number of information systems that process PII that were authorized or reauthorized to operate during the reporting period. <sup>25</sup>	2,749	415
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. <sup>26</sup>	63%	90%
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. <sup>27</sup>	61%	60%
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. <sup>28</sup>	62%	56%
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. <sup>29</sup>	61%	67%

<sup>25</sup> Federal agencies are required to provide oversight of information systems used or operated by contractors and other entities on behalf of the Federal Government, including ensuring that these information systems are included in their respective inventory of information systems. See OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix II § 4(j)(2)(c) (July 28, 2016).

<sup>26</sup> See *id.* at Appendix I § 4(a)(2), 4(e)(7).

<sup>27</sup> 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).

<sup>28</sup> See *id.* at Appendix I § 4(3).

<sup>29</sup> 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**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency has a policy that includes explicit criteria for analyzing the privacy risks when considering IT investments. <sup>30</sup>	79%	61%
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. <sup>31</sup>	75%	65%
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.

<sup>30</sup> See *id.* at § 5(d)(3).

<sup>31</sup> See *id.* at § 5(a)(3)(e)(ii).

**Table 9 Privacy Impact Assessments**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
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.	4,475	701
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. <sup>32</sup>	3,499	574
The agency has a written policy for privacy impact assessments that includes: <sup>33</sup>		
A requirement that a PIA be conducted and approved prior to the development, procurement, or use of an IT system that requires a PIA. <sup>34</sup>	100%	98%
A requirement that system owners, privacy officials, and IT experts participate in conducting PIAs. <sup>35</sup>	100%	93%
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. <sup>36</sup>	100%	95%
The agency has a process or procedure for each of the following: <sup>37</sup>		
Assessing the quality and thoroughness of each PIA.	96%	75%
Performing reviews to ensure that appropriate standards for PIAs are maintained.	96%	79%
Monitoring the agency’s IT systems and practices to determine when and how PIAs should be updated.	96%	75%
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%	75%

<sup>32</sup> Federal agencies are required to update PIAs whenever changes to the information technology, changes to the agency’s practices, or other factors alter the privacy risks associated with the use of such information technology. For the purposes of this question, an up-to-date PIA is a PIA that reflects any changes to the information technology, changes to the agency’s practices, or other factors that 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).

<sup>33</sup> See *id.* at Appendix II § 5(e) (July 28, 2016).

<sup>34</sup> N/A responses are not included in the percentages.

<sup>35</sup> See *id.*

<sup>36</sup> See *id.*

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

## F. Workforce Management

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

**Table 10 Workforce Management**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency ensures that its privacy workforce has the appropriate knowledge and skill. <sup>38</sup>	96%	93%
The agency assessed its hiring, training, and professional development needs with respect to privacy during the reporting period. <sup>39</sup>	88%	89%
The agency has developed a workforce planning process to ensure that it accounts for its privacy workforce needs. <sup>40</sup>	79%	68%
The agency has developed a set of competency requirements for privacy staff, including program managers and privacy leadership positions. <sup>41</sup>	75%	63%

**Table 11 Training and Accountability**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency maintains a mandatory agency-wide privacy awareness and training program for all Federal employees. <sup>42</sup>	100%	91%
The agency provides role-based privacy training to Federal employees with assigned privacy roles and responsibilities, including	75%	53%

<sup>38</sup> See *id.* at § 5(c)(2)

<sup>39</sup> See *id.* at § 5(c)(6).

<sup>40</sup> See *id.* at § 5(c)(1).

<sup>41</sup> See *id.*

<sup>42</sup> See *id.* at Appendix I § 4(h)(1).

managers, before authorizing access to Federal information or information systems. <sup>43</sup>		
The agency has measures in place to test the knowledge level of information system users in conjunction with privacy training. <sup>44</sup>	92%	81%
The agency has established rules of behavior, including consequences for violating rules of behavior, for Federal employees that have access to Federal information or information systems, including those that process PII. <sup>45</sup>	100%	95%
Among the agencies that have established rules of behavior, the agency ensures that Federal employees have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to access being granted. <sup>46</sup>	100%	93%

**Table 12 Contractors and Third Parties**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
The agency maintains a mandatory agency-wide privacy awareness and training program for all contractors. <sup>47</sup>	100%	89%
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. <sup>48</sup>	100%	95%
Among the agencies that have established rules of behavior, the agency ensures that contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access. <sup>49</sup>	100%	94%
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. <sup>50</sup>	0%	5%

<sup>43</sup> See *id.* at Appendix I § 4(h)(5).

<sup>44</sup> See *id.* at Appendix I § 4(h)(1).

<sup>45</sup> See *id.* at Appendix I § 4(h)(6).

<sup>46</sup> See *id.* at Appendix I § 4(h)(7).

<sup>47</sup> See *id.* at Appendix I § 4(h)(1)-(2), (4)-(7).

<sup>48</sup> See *id.* at Appendix I § 4(h)(6).

<sup>49</sup> See *id.* at Appendix I § 4(h)(7).

<sup>50</sup> See *id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).

Processes do not exist.		
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	4%	35%
Processes are fully documented and implemented and cover all relevant aspects.	38%	30%
Processes are fully documented and implemented and cover all relevant aspects and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current.	58%	30%
The extent to which the agency ensures appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information. <sup>51</sup> Processes do not exist.	0%	2%
Processes exist; however, they are not fully documented and/or do not cover all relevant aspects.	4%	23%
Processes are fully documented and implemented and cover all relevant aspects.	33%	37%
Processes are fully documented and implemented and cover all relevant aspects and reviews are regularly conducted to assess the effectiveness of the processes and to ensure that documented policies remain current.	63%	39%

## 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.<sup>52</sup>

<sup>51</sup> See *id.* at Appendix I § 4(j)(2)(a).

<sup>52</sup> See OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, § VII (Jan. 3, 2017).

**Table 13 Incident Response**

<b>FY 2019 – SAOP FISMA Performance Measures</b>	<b>CFO</b>	<b>Non-CFO</b>
Among the agencies that have a breach response plan, the agency has a breach response plan that includes the agency’s policies and procedures for each of the following: <sup>53</sup> Reporting a breach <sup>54</sup>	100%	98%
Investigating a breach <sup>55</sup>	100%	100%
Managing a breach <sup>56</sup>	100%	96%
Among the agencies that have a breach response plan, the SAOP reviewed the agency’s breach response plan during the reporting period to ensure that the plan was current, accurate, and reflected any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology. <sup>57</sup>	100%	96%
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. <sup>58</sup>	96%	89%
Among the agencies with a breach response team, all members of the agency’s breach response team participated in at least one tabletop exercise during the reporting period. <sup>59</sup>	74%	53%
The number of breaches, as OMB Memorandum M-17-12 defines the term “breach,” that were reported within agencies during the reporting period. <sup>60</sup>	18,175	823
The number of breaches, as OMB Memorandum M-17-12 defines the term “breach,” that agencies reported to US-CERT during the reporting period. <sup>61</sup>	9,226	96

<sup>53</sup> See *id.* at § VII, XI.

<sup>54</sup> N/A responses not include in the percentages.

<sup>55</sup> See *id.*

<sup>56</sup> See *id.*

<sup>57</sup> See *id.* at § X.B, XI.

<sup>58</sup> See *id.* at § VII.A, XI.

<sup>59</sup> See *id.* at § X.A, XI.

<sup>60</sup> See *id.* at § III.C, XI.

<sup>61</sup> See *id.* at § VII.D.1, XI.

The number of breaches, as OMB Memorandum M-17-12 defines the term “breach,” that agencies reported to Congress during the reporting period. <sup>62</sup>	3,014	1
The total number of individuals potentially affected by the breaches reported to Congress during the reporting period. <sup>63</sup>	3,783,642	29,700 <sup>64</sup>

---

<sup>62</sup> See *id.* at § VII.D.3, XI.

<sup>63</sup> See *id.* at § XI.

<sup>64</sup> Two other non-CFO agencies provided numerical responses to this question; however, both of those agencies responded they did not have any breaches that they reported to Congress.

# Section III: FY 2019 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<sup>65</sup>

This independent narrative section allows IGs (or independent assessors)<sup>66</sup> 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 2019 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)
- **Detect** (Intrusion Detection and Prevention; Exfiltration and Enhanced Defenses)

---

<sup>65</sup> 44 USC § 3553(c)(3) requires a summary of the independent evaluations; a summary of the IG/independent assessment can be found in each agency’s one-pager.

<sup>66</sup> 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.

- **Respond and Recover**<sup>67</sup>

Agency ratings fall within the following schema:

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

## 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 2019 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.

---

<sup>67</sup> Revisions to FY 2018 CIO metrics reduced the number of metrics in the Respond and Recover framework functions. Due to this reduction in number and the interconnectedness, these post-incident functions have been combined into a single area of assessment for the purposes of the RMAs.

**Table 14 IG Assessment Maturity Levels**

---

<b>NIST Cybersecurity Framework Function</b>	<b>Median Rating</b>
Identify	<i>Consistently Implemented</i>
Protect	<i>Consistently Implemented</i>
Detect	<i>Consistently Implemented</i>
Respond	<i>Consistently Implemented</i>
Recover	<i>Consistently Implemented</i>

---

Pursuant to 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 2019 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 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](https://www.performance.gov).

**Table 15 FY 2018 - FY 2019 CAP Goal Summary**

CAP Goal Metric	Target	Number of Agencies Meeting Target		Average Implementation*	
		FY 2018	FY 2019	FY 2018	FY 2019
<b>Manage Asset Security</b>					
Hardware Asset Management	95%	71	73	64%	70%
Software Asset Management	95%	56	70	58%	75%
Authorization Management	100%	79	81	91%	94%
Mobile Asset Management	95%	78	89	96%	99%
<b>Limit Personnel Access</b>					
Privileged Network Access Management	100%	56	58	94%	96%
High Value Asset System Access Management**	90%	58	66	70%	75%
Automated Access Management	95%	63	67	63%	88%
<b>Protect Networks and Data</b>					
Intrusion Detection and Prevention	4 of 6	45	60	N/A	N/A
Exfiltration and Enhanced Defenses	90%	66***	79	N/A	N/A
Data Protection	3 of 6	67	75	N/A	N/A

Source: Metrics as described in Appendix A of [FY 2019 FISMA CIO Metrics](#).

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

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

\*\*\* In FY 2018 the vast majority of agencies (93, including all 23 civilian CFO Act agencies) had met 3 of the 4 original targets set in the Exfiltration and Enhanced Defenses CAP goal and OMB considered this target to be achieved. As a result, the target was shifted to the remaining metric concerning exfiltration detection (FISMA CIO Metric 3.8). This number represents the represents the number of agencies meeting the new target in FY 2018.

## B. FY 2019 Information Security Incidents

### US-CERT Incidents by Attack Vector<sup>68</sup>

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 2019 FISMA Report captures incidents in accordance with US-CERT's [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.<sup>69</sup>

Table 16 highlights 28,581 incidents reported by Federal agencies, and validated with US-CERT, across nine attack vector categories. This represents an 8% decrease from FY 2018, when agencies reported 31,107 incidents. Improper Usage was the most common vector with 12,507 incidents occurring in the past year. The prevalence of this incident vector indicates that agencies have processes or capabilities that detect when a security policy is being violated, but lack automated enforcement or prevention mechanisms. Moreover, nearly 25% 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.

### Major Incidents

Of the 28,581 incidents reported in FY 2019, three incidents were determined by agencies to meet the threshold for major incidents in accordance with the definition in [OMB Memorandum M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements](#). A summary these major incidents is provided below, as well as their rating on the [CISA Cyber Incident Scoring System](#):

#### Department of Homeland Security

On December 3, 2019, DHS declared a major incident after determining that the Federal Emergency Management Agency (FEMA) National Emergency Management Information System Information Assurance (NEMIS-IA) system continued to send sensitive PII of disaster victims to a contractor responsible for meeting temporary shelter needs long after it was no longer required. FEMA took immediate steps to mitigate the incident by discontinuing the

---

<sup>68</sup> 44 USC § 3553(c)(1).

<sup>69</sup> NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide* lists common vectors that are the method of 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>

unnecessary sharing of PII with the contractor. Furthermore, a DHS-FEMA joint assessment team conducted a security assessment to revise the architecture of the system to meet the requirements of the DHS Sensitive Systems Policy Directive. An estimated 2.5 million hurricane survivors were impacted. The impact of this breach is Low (Green).

On January 31, 2019, DHS declared a major incident after determining potential unauthorized sharing of disaster survivors' PII by FEMA with a third-party volunteer organization. The organization had an approved Information Sharing Access Agreement (ISAA) with FEMA, but the agreement did not cover several data elements. FEMA amended the FEMA-State Agreement with the State of Texas on February 7, 2019, to further clarify that the third-party organization should have the same level of access these data elements as the State. An estimated 895,000 individuals were impacted. The impact of this breach is Minimal (blue).

On June 3, 2019, DHS declared a major incident following a ransomware attack at a contractor that manufacturer's license plate readers (LPR) utilized by U.S. Customs and Border Protection (CBP) at multiple US Border Patrol check points across the United States. CBP learned the contractor had taken unauthorized copies of images collected by CBP to their company network. The copied files included license plates images and facial images of the profile and front of travelers inside of a vehicle. These images were subsequently exfiltrated during the cyberattack on the company. The impact of this breach is Negligible (White).

**Table 16 Agency-Reported Incidents by Attack Vector**

Attack Vector	FY 2018			FY 2019		
	CFO*	Non-CFO*	Gov-wide	CFO	Non-CFO	Gov-wide
 <b>Attrition</b> An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	150	13	163	327	5	332
 <b>E-mail/Phishing</b> An attack executed via an email message or attachment.	6,558	372	6,930	4,102	286	4,388
 <b>External/Removable Media</b> An attack executed from removable media or a peripheral device.	32	0	32	46	1	47
 <b>Impersonation/Spoofing</b> An attack involving replacement of legitimate content/services with a malicious substitute.	44	3	47	35	0	35
 <b>Improper Usage</b> Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	9,360	314	9,674	12,280	227	12,507
 <b>Loss or Theft of Equipment</b> The loss or theft of a computing device or media used by the organization.	2,252	300	2,552	1,685	200	1,885
 <b>Web</b> An attack executed from a website or web-based application.	3,261	71	3,332	1,933	49	1,982
 <b>Other / Unknown</b> An attack method does not fit into any other vector or cause of attack is unidentified.	8,070	215	8,285	7,006	234	7,240
 <b>Multiple Attack Vectors</b> An attack that uses two or more of the above vectors in combination.	90	2	92	158	7	165
<b>Total</b>	<b>29,817</b>	<b>1,290</b>	<b>31,107</b>	<b>27,572</b>	<b>1,009</b>	<b>28,581</b>

\* The FY 2018 incident count summary incorrectly counted the Small Business Administration as a Non-CFO Act agency, this has been corrected in the numbers which appear above. The total number remains unchanged.

## **C. Agency Cybersecurity Performance Summaries**

# 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  
VDP – Vulnerability Disclosure Policy

# FY2019 Annual Cybersecurity Performance Summary

## Advisory Council on Historic Preservation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

2019 Infrastructure Operations and Cybersecurity Operations Maturity Improvements:

**Vulnerability and Asset Management:** Daily scanning and vulnerability assessments, real-time network mapping, and exploit checking capabilities were implemented. Remediation is a manual process, which is being automated.

**Threat Intelligence and Assessment:** Real-time and retroactive checks of network traffic against computer-telephony integration data feeds using both automated and manual processes were implemented.

**Security Monitoring:** Operationalized collection and analysis of full network packet flows, data feeds, logs, and alerts, and escalation of indications are done through combination of SIEM and cloud security products on networks and endpoints.

**Analysis and Detection:** Automated threat analytics and detection on network traffic and endpoints was implemented. Threats are correlated to threat intelligence and rules, prioritized using threat scores. Manual analysis is performed on high score alerts for investigation and validation, with automation playbooks in development.

**Incident Management and Response:** Active incident management processes were put in place. Alerts are monitored throughout the day, seven days a week. Potential incidents are monitored for mitigation before success. Incidents are addressed within several hours. Due to proactive monitoring, no successful major incidents occurred.

**Situational Awareness:** Tactical understanding of situations was improved. Correlation to mission and business impact awareness is available. Executive level support exists for cybersecurity program.

**Authentication:** Multi-factor cryptographic device authentication is being improved from one-time password authentication.

**Automation:** Significant efforts are underway to implement an orchestration and automation platform. The agency's limited security staff will be augmented using automation for enrichment, incident response, and automated remediation actions.

### 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 2019, 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 2020.

# FY2019 Annual Cybersecurity Performance Summary

## African Development Foundation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	2	0	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2</b>	<b>0</b>	<b>1</b>

### 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 DHS's CDM program. USADF performs an annual security and risk assessment on its information system resources according to the NIST Standard Publication guidelines and in compliance with FISMA. 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 DNS sink-holing and Cloud Email filtering as part of its effort to mitigate and reduce cybersecurity risk exposure. Even though USADF has embraced these efforts in managing risks, challenges still exist.

USADF has implemented a Risk Management Plan that covers risk management of all USADF information system resources which are categorized based on the business function, threat exposure, vulnerabilities and data type. Strategies for risk remediation are proportionate to the risks to the information system resources. The major constraints in resolving or mitigating risks are budgets and human resources. Senior management is addressing these constraints to make cybersecurity risk management and mitigation a priority at USADF.

USADF's senior management is fully engaged in reviewing risk analysis results and reports and supports the ongoing efforts of USADF's cybersecurity risk management strategy and processes. USADF's CISO ensures active involvement of information system owners, common control providers, CIOs, senior managers, designated authorizing officials, and other roles in the management of information system related cybersecurity risks.

### Independent Assessment

USADF's information security program was evaluated as part of the FY2019 FISMA Audit. This audit included an evaluation of the entire population of seven FISMA reportable systems at USADF. The FY2019 FISMA Audit noted 79 of 84 selected NIST SP 800-53, Revision 4 security controls were properly implemented. This along with the maturity of USADF's information security program led to the determination of USADF having an overall effective information security program. There were a few recommendations made to help USADF improve their information security program. These recommendations can be found in the FY2019 FISMA Audit report.

# FY2019 Annual Cybersecurity Performance Summary

## American Battle Monuments Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	0	1	1
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	0	1	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	2	1	5
			Multiple Attack Vectors	1	0	0
			<b>Total</b>	<b>3</b>	<b>3</b>	<b>6</b>

### CIO Self-Assessment

In 2019, the CIO identified 8 risks on the ERM risk register:

- 1-Risks on current Network Infrastructure
- 2-Loss of Integrity of ABMC Database
- 3-Lack of Mature and Tested Contingency Planning
- 4-Lack of IT Training for Users and Role Based Training
- 5-Loss of IT Personnel
- 6-Effects of Alternate or Shadow IT
- 7-Lack of Policies, Procedures and System Documentation
- 8-Cloud Vendor Lock-in and Vendor specific risks in the context of the Cloud migration

Risk 1 is being controlled through the on-going IT Modernization initiative.

Risk 2 has been mitigated by migrating the ABMC Database and Website to a new hosting service in June 2019. Also, a major database redesign is being planned in FY20.

ABMC is addressing Risk 3 and will be developing a contingency plan in FY20.

Risk 4 is being addressed in FY20 by the IT Team.

Risk 5 is mitigated by recruiting IT team members and adding external resources.

Risk 6 is mitigated by establishing additional administrative and technical controls as part of the Modernization project.

Risk 7 is being mitigated by additional Cybersecurity resources working on documentation, policies and procedures. The Security and Compliance capability from the Cloud Security provider will streamline control requirements and provide visibility to compliance.

Risk 8 is being accepted by ABMC.

### Independent Assessment

Overall ABMC has an effective information security program in place that not only addresses FISMA requirements, but also meets the business needs of ABMC.

ABMC as an organization historically has lacked documentation of policies and procedures. This known issue has created many of the results noted in our FISMA evaluation. This issue has been and is being aggressively addressed by ABMC management.

ABMC has identified a multitude of POAMs to address identified FISMA issues and ABMC has made addressing FISMA requirements one of their highest priorities in the organization. ABMC has an information security program that continues to mature. ABMC's overall information security program needs to grow from an overall consistently implemented (level 3) status to a managed or measurable maturity (level 4).

ABMC's information security program needs improvement in the following areas:

- Information security policies and procedures;
- Contingency Planning

The scope of this evaluation covered ABMC agency-owned and contractor-operated information systems of record as of September 30, 2019.

# FY2019 Annual Cybersecurity Performance Summary

## Armed Forces Retirement Home

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	0	0
Detect	At Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The Armed Forces Retirement Home (AFRH) in coordination with the Department of Interior - Office of the Chief Information Officer (DOI-OCIO) continue to strive to improve the organization's security posture by ensuring the right technologies and security controls are in place that reduce the organization's risk, as well as processes to monitor the effectiveness of the security program.

AFRH's main mission and strategy is to provide residences and related services for retired and former members of the Armed Forces. As a "defend in place" continuing care facility their core responsibility is the care and safety of their residents and personnel. The objective of the Security Program is to create effective administrative, technical and physical safeguards in order to protect critical data and resources. AFRH has seen significant improvements in the past year, some clear successes are listed as follows: the successful implementation of multi-factor authentication mechanisms across the agency utilizing PIV technology; the update and documentation of the System Security Plan to NIST Rev4; the scheduling, completion and review of monthly security scans; annual contingency planning and testing; annual Security Risk Assessments conducted to ensure safeguards are implemented uniformly and; the closing of several outstanding Plan of Action and Milestones (POA&M's) as part of the continuous monitoring program.

Moving forward, AFRH will continue to:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
- Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

### Independent Assessment

The information security program of AFRH was evaluated as effective. AFRH Risk Management methodology for assessing FISMA compliance was a business-driven process to identify the effectiveness of its Security Program through IT assessments, continuous monitoring practices and an analysis of policies and procedures to validate the operational practices for the following FISMA control domains:

- Risk Management
- Identity and Access Management
- Privacy
- Configuration Management
- Contingency Planning and
- ICSM

# FY2019 Annual Cybersecurity Performance Summary

## Barry Goldwater Scholarship and Excellence in Education Foundation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	NA	NA	0
Protect	At Risk	Ad Hoc	E-mail	NA	NA	0
Detect	At Risk	Ad Hoc	External/Removable Media	NA	NA	0
Respond		Ad Hoc	Impersonation	NA	NA	0
Recover	Managing Risk	Ad Hoc	Improper Usage	NA	NA	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	NA	NA	0
			Web	NA	NA	0
			Other	NA	NA	0
			Multiple Attack Vectors	NA	NA	0
			<b>Total</b>			<b>0</b>

### CIO Self-Assessment

The Barry Goldwater Foundation is a small agency with two permanent federal employees and does not have an in-house IG or CIO. The Foundation's IT inventory consists of two desktop computers, two laptop computers, and two printers for general office applications. The computers and data are password protected and are not connected to any government network. An approved contractor provides support for the Foundation's scholarship program and is a separate entity from the Foundation. In coordination with, GSA, USDA/OCFO, and the website/program contractor, the Foundation has implemented security measures necessary to safeguard its limited resources.

### Independent Assessment

The information security program of the Barry Goldwater Foundation was evaluated as effective. The Goldwater Foundation is a small agency with two permanent federal employees and no in-house IG or CIO. The Foundation's IT inventory consists of two desktop computers, two laptop computers, and two printers for general office applications. The computers and data are password protected and are not connected to any government network. An approved contractor provides support for the Foundation's scholarship program and is a separate entity from the Foundation. In coordination with, GSA, USDA/OCFO, and our website/program contractor, the agency has implemented security measures necessary to safeguard its limited resources.

# FY2019 Annual Cybersecurity Performance Summary

## Board of Governors of the Federal Reserve

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	1	0
Protect	Managing Risk	Managed and Measurable	E-mail	1	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Managed and Measurable	Improper Usage	1	0	1
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	5	1	2
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>7</b>	<b>2</b>	<b>3</b>

### CIO Self-Assessment

Primary cybersecurity risks to the Federal Reserve Board (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;
- Completed implementation of two-factor PIV authentication for all users
- Enforcement of two-factor PIV authentication for all users (privileged and non-privileged);
- Enhanced monitoring of user behavior
- 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; and
- Multiple third-party assessments beyond the work done by the Office of Inspector General.

In 2019, areas of focus to further enhance our protections include:

- Implementation of the DHSCDM program;
- Continuous enhancement of network and user behavior monitoring;
- Enhancement of anti-phishing controls; and
- Enhancement of the insider threat program.

### Independent Assessment

Overall, independent assessment found that the Board's information security program is 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, the assessment identified opportunities to strengthen processes and controls in the areas of risk management, identity and access management, and data protection and privacy to further mature the program and ensure that it remains effective. The OIG audit report includes six recommendations to strengthen controls in these areas.

# FY2019 Annual Cybersecurity Performance Summary

## Chemical Safety Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	0	0	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The CSB has configured multifactor authentication (MFA) for network access. An authentication server is installed on multiple servers for redundancy. It is configured to synchronize and validate credentials on premises and in the cloud and send a two-factor authentication code during password login to the CSB user's mobile device, via either an app or a numeric code in a text message. The method can be set by the global administrator; it is also possible to configure the system to allow the user to choose the method at each login. Two-factor authentication can be enabled and enforced for login to the CSB's cloud sharing site remote access by VPN; and webmail.

Multi-factor authentication is currently enabled and enforced for administrator accounts (users on the IT staff with access to domain admin accounts) connecting to the CSB's SharePoint site in the Microsoft cloud and remote access by VPN. User accounts can be enabled and enforced as well by a simple step in the Azure MFA management console. Two-factor authentication is monitored and logged by the system so that logins can be tracked and verified. The CSB will continue to test this process with the administrator accounts and expects to begin phasing in multifactor authentication with a test group of a few employees in each department by the end of calendar year 2019, with full implementation in the first quarter of 2020.

### Independent Assessment

The information security program of CSB was evaluated as effective. CSB has demonstrated it has defined policies, procedures and strategies for all five of the information security function areas. The Office of the Inspector General assessed the five Cybersecurity Framework function areas and concluded that CSB has achieved an overall maturity Level 2, Defined, which denotes that the agency has formalized documented policies, procedures and strategies, in adherence to the FY 2019 Inspector General FISMA reporting metrics.

While CSB has policies, procedures and strategies for these function areas and domains, improvements are still needed in the following areas:

Risk Management - CSB neither identified nor defined its risk management procedures for identifying, assessing or managing supply chain risk.

Incident Response - CSB did not define incident handling processes specific to eradication in its incident response procedures.

Identity and Access Management - CSB has not completed its corrective actions to implement processes for the use of PIV cards for the logical access of privileged and non-privileged users.

# FY2019 Annual Cybersecurity Performance Summary

## Commission of Fine Arts

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	High Risk	Ad Hoc	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	Managing Risk	Ad Hoc	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
			Web	2	0	0
			Other	0	0	0
			Multiple Attack Vectors	2	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>4</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The CFA's IT systems and security posture remain unchanged since it submitted its 2018 FISMA report with no adverse cybersecurity incidents to report. The most significant identified cybersecurity risk remains the absence of knowledgeable and dedicated IT and cybersecurity staff, or access to such staff in other agencies, with the capacity and expertise to fully address the CFA's cybersecurity infrastructure.

Nevertheless, the CFA endeavors to manage and mitigate risks to the best of its capacity. The Agency has completed requirements gathering and Statements of Work for an updated MTIPS service, in advance of expiring contracts and in anticipation of implementing OMB Memorandum M-19-26, Update to the Trusted Internet Connection (TIC) Initiative. The CFA has been accepted into DHS's CDM DEFEND task order, participated in a kick-off meeting and is actively working with DHS to plan and implement the CDM initiative in conjunction with the MTIPS upgrade.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Commission of Fine Arts was not performed for FY 2019, 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 CFA will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Commission on Civil Rights

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	At Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The United States Commission on Civil Rights (USCCR) relies extensively on IT resources to accomplish its mission and continues to take positive steps for improving its security posture. USCCR made some improvements in the agency's IT Modernization plan by upgrading its legacy network and adding tools to assist in becoming fully compliant with BOD-18-01. USCCR has a similar risk profile to other small, internet enabled agencies that have had significant success adopting cloud-based services. USCCR continues to attempt to align its IT strategy with OMB and the President's Management Agenda by focusing on utilizing interagency shared services, such as cloud SaaS and IaaS models. USCCR acknowledges that it must reduce its unsupported software to remove vulnerabilities and better manage the use of non-standard software. In FY2020, USCCR hopes to continue implementing the IT Modernization Plan to increase its maturity.

### Independent Assessment

To meet FISMA requirements USCCR contracted with an independent auditor to conduct the FY 2019 independent evaluation of its information security program and practices as a performance audit under Generally Accepted Government Auditing Standards. The auditors concluded that overall, 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 plans of action and milestones (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 FY2020.

# FY2019 Annual Cybersecurity Performance Summary

## Commodity Futures Trading Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	1	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	1	1	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	1	0	0
			Loss or Theft of Equipment	0	0	2
			Web	0	0	0
			Other	2	2	2
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>5</b>	<b>3</b>	<b>4</b>

### CIO Self-Assessment

CFTC has built an Information Security Program to address the growing threat landscape, with a balanced mix of policy and compliance activities to govern the protection of its data, assets and mission functions. Recently identified risks include weaknesses related to internal controls; specifically, identity access management, continuous monitoring, and data recovery. The Commission also needs to improve on the timely remediation of security vulnerabilities in its infrastructure. Furthermore, efforts should focus on establishing effective processes to resolve outstanding security risks as documented in the POA&M management system. Key gaps that have been identified in our information security program include:

- Fulfillment of DHS CDM program dependencies.
- Timely remediation of POA&Ms 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.
- Adopt the Federal Cloud Smart strategy to accelerate secure migration to the cloud.

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 the Commission carefully examine the effects and apply best practices to provide timely, reliable, and secure IT services. The CFTC cybersecurity program requires a commitment in the investment of people, processes, technology, and capital to provide information assurance and computer network defense for our mission critical systems and data.

### Independent Assessment

For the reporting period, CFTC's IT security program was rated as "Effective" using CIGIE's and DHS' maturity evaluation tool. It was recommended that Office of Data and Technology (ODT) management:

- Take action on FY 2019 Penetration Test Vulnerabilities identified as High, Medium, and consider Low vulnerabilities for remediation action.
- Develop periodic functional data restore tests and schedule taking into account business system criticality.

Additionally, prior year recommendations were evaluated from the FY 2017, and FY 2018 FISMA performance audits and all recommendations were closed.

# FY2019 Annual Cybersecurity Performance Summary

## Consumer Financial Protection Bureau

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	2	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	3	3	3
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	120	151	100
			Web	6	0	0
			Other	13	10	0
			Multiple Attack Vectors	2	0	1
			<b>Total</b>	<b>146</b>	<b>164</b>	<b>104</b>

### CIO Self-Assessment

Since the Bureau was established in 2011, CFPB has taken an innovative approach to fulfill its mission to serve the American consumer by continuing to leverage digital and cloud technologies. While the journey to become a modern agency has presented opportunities for efficiency and innovative services, it has not come without challenges. CFPB uses internal security controls assessments, continuous monitoring, advanced technical capabilities, innovative security training, and audits to identify cyber risks and opportunities to gain efficiencies in operations that enhance mission effectiveness and reduce enterprise risk. The results of these activities are further analyzed to help inform decisions that consider: 1) enhancing visibility into the data and assets that need to be protected in a distributed IT environment in a way that embraces the shared service models of FedRAMP and federal service providers; 2) addressing the data protection needs of the organization focused on the Bureau's most valuable IT assets, while not hindering CFPB's ability to interface with the public or limiting the Bureau's mission; 3) achieving near real-time situational awareness to cyber threats and vulnerabilities; 4) safeguarding sensitive information; and 5) making consumer data available to carry out CFPB's mission. During its formation, CFPB seized the opportunity to establish a cost-effective, risk-based strategy to implement the NIST Risk Management Framework (RMF) and manage cybersecurity risks. In 2019, the CFPB worked to mature its risk-based approach to security, integrating the broader agency approach to enterprise risk management activities.

### Independent Assessment

Overall, we found that the Bureau's information security program is operating effectively at a level-4 (managed and measurable) maturity. For instance, the Bureau's information security continuous monitoring and incident response processes are effective and operating at a level 4. However, we identified further opportunities to strengthen processes and controls in the areas of risk management, identity and access management, data protection and privacy, incident response and contingency planning to ensure that its information security program remains effective. Our 2019 FISMA audit report includes seven recommendations to strengthen controls in these areas.

# FY2019 Annual Cybersecurity Performance Summary

## Consumer Product Safety Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	1	0	0
Protect	At Risk	Ad Hoc	E-mail	4	1	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	1	0	3
			Loss or Theft of Equipment	0	5	1
			Web	2	0	0
			Other	7	2	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>15</b>	<b>8</b>	<b>5</b>

### CIO Self-Assessment

Throughout FY 2019 CPSC worked diligently to reduce agency cyber risk and has continued to make significant improvements in the IT security program. While opportunities for improvement were noted in the annual FISMA assessment overseen by the OIG, CPSC made significant progress in many of the areas identified. CPSC maintained a hardware and software inventory; documented and implemented baseline configurations, increased the timeliness of security patching through the implementation of an automated patch management solution; consistently enforced PIV based two-factor authentication or other NIST Level of Assurance (LOA) 4 credential; applied the principle of least privilege to the extent practical given limitations in staffing resources and expanded logging to increase accountability; updated and enhanced the CPSC Business Impact Assessment (BIA); updated and tested all agency system contingency plans; updated and enhanced the agency business impact assessment; provided mandatory IT security and privacy training to include a phishing exercise to 100% of agency personnel and expanded role based training to include all managers and executives; advanced the agency enterprise risk management program, and made improvements to and increased staffing for the agency's privacy program.

Additional areas of focus during FY 2019 included:

- full implementation of all DHS EINSTEIN tools to detect and block attacks;
- updates to all System Security Plans (SSP) and Authorities to Operate (ATO);
- improvements to agency networks to support improved network access control and;
- progress in the implementation of CDM, improvements to processes associated with configuration controls and authorizations.

### Independent Assessment

The information security program of the CPSC was evaluated as not effective. CPSC improved its policies and procedures, implemented new cybersecurity solutions, and is actively working toward standardizing its risk documentation. These improvements resulted in the achievement of Level 4, Managed and Measurable, for the ISCM (Detect) and Incident Response (Respond) functions on the FISMA maturity model. 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
- implemented processes to adequately protect PII throughout the data lifecycle
- ensured information technology contracts and agreements for goods and services included the required Federal Acquisition Regulation clauses and/or other provisions

# FY2019 Annual Cybersecurity Performance Summary

## Corporation for National and Community Service

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	2	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	1	3
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	4	1	0
			Web	1	0	0
			Other	6	0	3
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>13</b>	<b>2</b>	<b>6</b>

### CIO Self-Assessment

CNCS continues to make improvements in addressing cybersecurity risks. Specifically, CNCS has made progress in addressing the Credentialing and Authorization security domain. During this reporting period CNCS was able to implement multifactor authentication (MFA) for 63% of network general users as part of its technical upgrade. CNCS has a goal to have all general users using MFA by the end of FY 2020 Q3. CNCS will have CDM operational no later than end of FY 2020 Q2. CDM will help CNCS address the risk associated with monitoring the configuration and overall protection of its High Value Asset systems. CNCS is actively working to improve its remote connection and validation capability by changing its licensing options within cloud environments. The SaaS solution has a function that will enforce a specific security level for all remote connections to its environment. The additional capabilities will also address CNCS's ability to monitor all inbound and outbound traffic for unauthorized exfiltration. The future phases of CDM will help CNCS address real-time responses to security violations for HVAs.

### Independent Assessment

The information security program of CNCS has made little progress since last year, and it remains not effective. The maturity metrics for the eight domains and five security functions are largely unchanged. However, CNCS regressed in two of the domains and one of the function areas.

Control weaknesses leave CNCS vulnerable and may expose sensitive information, including PII, to unauthorized access and use. The CNCS network remains exposed to many critical and high-severity vulnerabilities stemming from unpatched software, improper configuration settings and unsupported software. CNCS began to implement multifactor authentication enterprise-wide but did not complete it by the conclusion of testing. Full implementation of multifactor authentication should improve CNCS's cybersecurity.

We again recommend that CNCS complete a strategic analysis of the government-wide metrics and the weaknesses identified in this evaluation, to develop a multi-year approach designed to realize steady, measurable improvements in information security in each of the domains and security function areas.

# FY2019 Annual Cybersecurity Performance Summary

## Council of the Inspectors General on Integrity and Efficiency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	Managing Risk	Ad Hoc	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond	At Risk	Ad Hoc	Impersonation	NA	0	0
Recover		Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	1	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>1</b>	<b>0</b>

### CIO Self-Assessment

Over the course of the year the Agency has addressed two important and complex projects. The first is deploying and implementing a Mobile Device Management solution. The Agency is currently using the Device Manager in combination with Office 365. Both provide the Agency a complete control of mobile devices. The second is procuring and implementing Centralized Log Management. This technology allows the Agency capturing logs from different types of devices including Active Directory and Server Audit logs. With such information the Agency has the capability of identifying suspicious behaviors, as well as producing security and compliance reports that will enhance the Agency's cyber-security posture.

### 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 2019, 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 CIGIE will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Court Services and Offender Supervision Agency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	0	3	1
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	Managing Risk	Defined	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	1	0
			Web	1	0	0
			Other	4	1	2
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>5</b>	<b>5</b>	<b>3</b>

### 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 continues to make 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 CSOSA was evaluated as not effective. Overall, the Agency (CSOSA and PSA) has made progress in addressing previously identified information security deficiencies. DHS, OMB, and the Council of the Inspectors General on Integrity and Efficiency considers Level 4, Managed and Measurable as an effective level at the metric, domain, function and overall security program. Based on the assessment of the Agency's information security program, the overall maturity level results at the metric level in-between Level 1 Ad Hoc, Level 2 Defined, and Level 3 Consistently Implemented.

# FY2019 Annual Cybersecurity Performance Summary

## Defense Nuclear Facilities Safety Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	1	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	2	3
			Web	0	0	0
			Other	1	0	1
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>2</b>	<b>2</b>	<b>4</b>

### CIO Self-Assessment

DNFSB continues to make improvements to help the agency mitigate remaining cybersecurity risks. The cybersecurity team has been expanded and a contractor has been engaged to update the GSS's SA&A package. Two cybersecurity tools were configured and staff was trained on their usage. The CSF protect function has progressed with the evaluation and approval to acquire a FedRAMP authorized Enterprise email solution to protect against phishing and spam as well as train all users continually throughout the year.

### Independent Assessment

The information security program of DNFSB was evaluated as effective. Improvements from last year include a 3rd-party risk assessment and Gap analysis. DNFSB has a good plan for the direction they want to go, but need another year to conduct proper Incident Response, COOP, and disaster-recovery exercises for its GSS. IT Operations and the CIO/CISO office need better transparency with continuous monitoring technology capabilities, which are being under-utilized.

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 some of its programs. In order to mature its programs, DNFSB should continue to make improvements to existing policies and procedures and develop and implement new policies and procedures in programs where there are none.

# FY2019 Annual Cybersecurity Performance Summary

## Denali Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
<b>Overall</b>	<b>At Risk</b>		Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### 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

An independent evaluation of the status of the IT cybersecurity program for the Denali Commission was not performed for FY 2019, 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 Denali Commission will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Agriculture

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	1	1
Protect	At Risk	Defined	E-mail	40	20	22
Detect	Managing Risk	Defined	External/Removable Media	0	1	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	413	323	223
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	182	9	4
			Web	226	161	157
			Other	464	365	227
			Multiple Attack Vectors	43	49	13
			<b>Total</b>	<b>1,368</b>	<b>929</b>	<b>647</b>

### CIO Self-Assessment

Cybersecurity risks to USDA originate from malicious actors that seek to exploit, degrade, or block access to the information technology solutions used to deliver cost-effective services and achieve the mission of USDA. To counter these risks, the OCIO information security program implemented many cybersecurity activities in FY19, which can be measured by:

- Improving the maturity rating of the information security program by 32% over FY18 as assessed by the Inspector General FISMA Reporting Metrics.
- Achieving 8 of 10 CAP Goals by the fourth quarter of FY19.
- Improving two Security Domain ratings from “At Risk” to “Managing Risk” and one Security Domain from “High Risk” to “Managing Risk” as measured by the OMB RMA report.

Specific achievements that reduced risk were made possible by:

- Streamlining cybersecurity management by realigning and consolidating cybersecurity functions and capabilities;
- Strengthening strategic IT governance by updating eight information security directives;
- Closing 26 data centers and approved Department-wide secure cloud services;
- Enabling a strategic approach to data management and introducing dashboards to support data-driven capabilities;
- Launching secure public facing applications and implementing DMARC on all public facing email applications;
- Implementing 18 OIG recommendations that were opened prior to FY18 and four recommendations from FY18 resulting in 12 closed audits; and
- Closing over 1,100 POA&Ms with 39% of the closures covering critical controls cited by the OIG in previous FISMA audits as contributing to an IT Security Material Weakness.

### Independent Assessment

The information security program of USDA was evaluated as not effective. The Department took some positive steps for improving the Department’s security posture in FY 2019. For example, a significant improvement was made to the incident response program through finalizing policies and procedures that govern the process. However, improvements are still needed for many functions. The Department consistently issues policies that delegate procedures and responsibilities for compliance to the agencies. While the Department does have tracking mechanisms, scorecards, and tools such as CSAM to aid in governance and oversight of some areas, there are still many areas 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 Departmental policies.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Commerce

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	15	4	14
Protect	At Risk	Defined	E-mail	567	660	330
Detect	Managing Risk	Defined	External/Removable Media	1	0	0
Respond		Defined	Impersonation	NA	2	2
Recover	At Risk	Defined	Improper Usage	407	582	722
			Loss or Theft of Equipment	131	67	29
			Web	210	196	59
			Other	655	305	284
			Multiple Attack Vectors	21	11	23
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2,007</b>	<b>1,827</b>	<b>1,463</b>

### CIO Self-Assessment

In FY19, the primary cybersecurity risks facing the DOC were the same as in FY18: lack of near-real time continuous monitoring to facilitate standardized risk-based cybersecurity management, including the ability to monitor the implementation of NIST SP 800-53 controls across all DOC environments, and enhanced security requirements across HVA systems, deficiencies in the timely identification and mitigation of vulnerabilities, and continued inability to hire staff with requisite skill sets needed to maintain security processes on DOC systems and environments. To mitigate these risks, the DOC continued to implement and mature multiple enterprise-wide initiatives including the phased deployment of the CDM program, which is currently addressing Phase 1 and 2 gaps in tools and capabilities, as well as Phase 3 “DEFEND” activities, including collaborating with the DOC’s subcomponents on supplemental scanning, monitoring, and patching capabilities. DOC continues the integration of CDM and Enterprise Continuous Monitoring and Operations (ECMO) program to improve continuous monitoring posture across the agency. The DOC continues to support the Enterprise Security Operations Center (ESOC) through use of CDM and other tools to support Incident Response, Management and information sharing across the DOC. In FY19, ESOC created the Commerce Threat Intelligence Portal, to facilitate the timely collection and distribution of threat intelligence and other important cybersecurity information. DOC released a new enterprise IT security policy, the IT Security Baseline Policy, which enhances security requirements to strengthen the DOC’s IT Security posture. The DOC also purchased an anti-phishing exercise tool to assist subcomponents in training employees on the attributes of a phishing attack. DOC continues to work with subcomponents to implement enhanced security controls on HVA systems. DOC facilitated one full DHS HVA RVA and Security Architecture Review SAR and two SAR-only assessments in FY19.

### Independent Assessment

The information security program of DOC was evaluated as not effective. The OIG completed an audit of the Department's FISMA compliance by assessing the effectiveness of the Department's information security program and practices. OIG also reviewed a representative subset of 12 IT systems from four of the Department'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 defined most of the needed policies and procedures. However, we found that the Department did not consistently implement its IT security policies and procedures.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Education

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	2	0
Protect	Managing Risk	Defined	E-mail	14	39	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	115	40	62
			Loss or Theft of Equipment	26	2	0
			Web	7	4	0
			Other	21	0	17
			Multiple Attack Vectors	4	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>187</b>	<b>87</b>	<b>79</b>

### CIO Self-Assessment

The Department of Education completed several activities associated with the NIST Cybersecurity Framework (CSF) Identify Security Function in the Metric Domain area of Risk Management.

The Department's CIO assumed responsibility as the Authorizing Official (AO) for all HVAs, High impact, and Moderate impact systems. This change in delegation of authority provides greater oversight of the Department's most important IT systems and allows for the Department's CIO to determine acceptable levels of risk for each system.

The Department completed several activities to improve the Protect Security Function in the Metric Domain areas of Security Training, Data Protection and Privacy, and Identity and Access Management.

ED, employed increasingly complex phishing scenarios and established administrative controls that enhance user awareness of the risks of cyber threats.

For the Detect Security Function in the ISCM Metric Domain, ED continues to make improvements to capabilities and efficiencies.

Working with DHS, the Department continued to mature our CDM implementation by incorporating additional program elements of the Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) series of task orders.

For the Respond Security Function in the Metric Domain of Incident Response, ED made improvements to increase capabilities and efficiencies while maintaining the security posture of the Department. ED improved SPAM filtering and anti-phishing policies through the Department's email service provider.

For the Recover Security Function Contingency Planning domain, ED created and provided a new service to ISOs and ISSOs by initiating quarterly Department-wide Contingency Plan Testing (CPT) and Incident Response Plan (IRP) tabletop exercise.

### Independent Assessment

Our objective was to determine whether the Department of Education's (Department) and Federal Student Aid's (FSA) overall information technology security programs and practices were effective as they relate to Federal information security requirements. We 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 reviewed in their operational environment. We found that the Department and FSA were not effective in any of the five security functions—Identify, Protect, Detect, Respond, and Recover. We also identified findings in all eight metric domains. The Department has made improvements on individual metric scoring (questions). The Department demonstrated improvement from FY 2018 within the metric areas 1) Security Training 2) Identity and Access Management 3) Configuration Management 4) Data Privacy and Protect 5) Contingency Planning and 6) Incident Response. The most significant change was in Risk Management. The overall maturity rating for the security function went from Consistently Implemented to Defined. This was due to the new requirements in this year's FY 2019 FISMA IG Metrics addressing the SECURE Technology Act provisions for supply chain management, as well as related policy and procedural requirements. Except for Risk Management, the overall FY 2019 maturity level rating was not impacted.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Energy

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Consistently Implemented	Attrition	4	1	3
Protect	At Risk	Consistently Implemented	E-mail	64	79	111
Detect	At Risk	Defined	External/Removable Media	0	0	1
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	102	172	231
			Loss or Theft of Equipment	167	191	157
			Web	75	42	29
			Other	131	161	287
			Multiple Attack Vectors	1	1	1
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>544</b>	<b>647</b>	<b>820</b>

### 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 of the Department.

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 working to combat these threats by focusing on strengthening enterprise situational awareness to foster near real-time risk management and defense against advanced persistent threats; forging interagency and sector partnerships to protect critical infrastructure; promoting information sharing, strengthening privacy protections; enhancing policy and guidance, and advancing technologies for cyber defenses through the creation of the Artificial Intelligence and Technology Office (AITO) that will focus on bringing new innovative approaches to the cyber arena.

DOE completed a rigorous review and revision of its cybersecurity policy, which addresses and requires the incorporation of risk management in both the enterprise and program office-level, to include laboratories, sites, and plants. Key updates include the requirement for Enterprise-wide cybersecurity risk management, supply chain risk management, and annual submissions of risk registers by each Departmental Element.

Additionally, DOE continues to participate in the DHS CDM program. As Phase I CDM tools are implemented across DOE, significant improvements in ISCM will be realized and will provide a holistic view of the security posture of the entire DOE enterprise.

### Independent Assessment

The Office of Inspector General (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 related to national security systems. Specifically, we reviewed the Department's progress towards meeting the DHS/OMB FISMA metrics at selected 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; and Respond. We found that the Department had achieved a Defined (Level 2) maturity level for the Detect and Recover functions. 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 and the Office of Enterprise Assessments. The rating for each of the metrics includes the results of both unclassified and national security system environments.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Health and Human Services

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Consistently Implemented	Attrition	14	14	19
Protect	Managing Risk	Consistently Implemented	E-mail	1,120	885	603
Detect	Managing Risk	Consistently Implemented	External/Removable Media	5	16	2
Respond		Consistently Implemented	Impersonation	NA	26	5
Recover	At Risk	Defined	Improper Usage	2,575	3,588	4,674
			Loss or Theft of Equipment	651	823	575
			Web	907	1,263	609
			Other	1,952	3,063	1,088
			Multiple Attack Vectors	72	0	33
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>7,296</b>	<b>9,678</b>	<b>7,608</b>

### CIO Self-Assessment

HHS took many steps in FY19 to mitigate cybersecurity risks to the agency, focusing on its high value assets (HVAs) and FISMA Cross-Agency Priority (CAP) goal performance, through collaboration & governance. HHS HVA PMO teamed with the HHS innovation office to offer operating divisions (OpDivs) crowd-sourced penetration testing via HHS' bug bounty program. This employs 3rd parties to assist in the identification of present and emerging vulnerabilities and remediation to protect against malicious activity. The HHS HVA PMO and Vulnerability & Penetration Testing team determined that capabilities exist to perform DHS' Risk and Vulnerability Assessment methodology using existing resources; planned pilots to occur in FY20. FY19 also saw collaboration with HVA PMO and HHS' Continuity Program. During HVA prioritization, HHS saw a significant overlap with its mission essential systems and HVAs. Both teams started to educate OpDivs on the relationship between mission essential functions and HVAs; encouraging closer engagement between Cybersecurity and Continuity teams. HHS completed its HVA policy update to align with the most recent OMB and DHS policies and encouraging the use of best practices such as the DHS HVA Control Overlay. HHS also formalized its ERM Framework and the HHS CISO is a member of the ERM Council.

In addition to HHS' HVA efforts, the HHS Office of the CIO (OCIO) collaborated with the OpDivs to improve our FISMA CAP goal performance. HHS OCIO focused its attention on improving the CIO FISMA metrics by identifying challenges and proposing solutions to meet the CIO FISMA CAP goals. As a result, in FY19 Q4, HHS met seven (7) of the 10 FISMA CAP goals; in FY18 Q4, HHS met five (5) of the 10 FISMA CAP goals. At HHS, meeting the CAP goals is a high priority. The HHS OCIO continues to discuss and implement plans to improve the CAP ratings.

### Independent Assessment

Based on the results of our evaluation, we determined that the HHS' 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 determined that HHS was "Consistently Implemented" in the Identify, Protect, Detect, and Respond areas. The FY19 FISMA audit reflects the assessment of 4 of the 12 HHS operating divisions (OpDivs) and not the entire agency. HHS is a federated environment which brings challenges in attaining a "Managed and Measurable" maturity model at all OpDivs. Overall, HHS made strides by implementing changes which strengthened the enterprise-wide information security program. HHS is cognizant of the opportunities which can strengthen its overall information security program and should help ensure that policies and procedures at all OpDivs are consistently implemented across its security programs. HHS continues to work towards implementing a Department-wide Continuous Diagnostics and Mitigation (CDM) program in coordination with DHS with the ultimate goals of continuous monitoring of HHS networks and systems, real-time reporting of OpDivs status and progress to help address and implement strategies to combat risk, prioritization of issues based on established risk criteria, and improving federal cybersecurity response capabilities. 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 using appropriate tools, processes, and controls at all OpDivs. HHS should also continue to build towards a working model where all the function areas interact with each other in real-time and provide holistic and coordinated responses to security events helping to strengthen all aspects of its information security program.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Homeland Security

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	2	0	1
Protect	Managing Risk	Managed and Measurable	E-mail	241	477	93
Detect	Managing Risk	Ad Hoc	External/Removable Media	13	9	10
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	407	143	544
			Loss or Theft of Equipment	16	14	15
			Web	124	64	30
			Other	1,245	420	379
			Multiple Attack Vectors	57	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2,105</b>	<b>1,127</b>	<b>1,072</b>

### CIO Self-Assessment

In Fiscal Year (FY) 2019, DHS received a “managing risk” rating from the Risk Management Assessment. In the Protect function, DHS continues to improve and expand the visibility of enterprise-wide cybersecurity risks by standardizing toolsets used to manage mobile assets and configurations from the CDM program. The implementation of CDM will mitigate this challenge, as there will be greater visibility and more frequent assessment into threats and vulnerabilities facing the entire Department. 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. In FY2019 the Protect function is rated “Managing Risk”, while it was rated “At Risk” in FY2018. DHS actively monitors Authority to Operate 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 procedures 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 monitoring of systems operating on DHS network. The Department has updated and communicated its Information Security Performance Plan for FY2020, allowing agency executives more visibility on IT risks impacting their mission space. DHS offered cybersecurity incentives in FY2019; the federal sector continues to face challenges in filling vacant cybersecurity positions primarily due to competing civilian entities that compete for industry skilled personnel. DHS Office of the Chief Information Officer, does not concur with the independent assessment carried out and reported by OIG as included in this report and the performance summary report.

### Independent Assessment

The information security program of DHS was evaluated as not effective. DHS does not have an effective strategy and organization-wide approach to manage its information security program. Without consulting the Department’s senior leadership or appropriate Congressional oversight committees, in June 2019 the DHS CIO decided to permit the Coast Guard to submit their cybersecurity and FISMA reports to the Department of Defense and to provide an information copy to DHS. The CIO’s decision is contrary to the statutory reporting requirements under FISMA 2014, OMB FY19 FISMA reporting instructions, and the terms stipulated in the Department’s senior leadership’s agreements with the Coast Guard and the Department of Defense. Further, OMB requires all Chief Financial Officer Act agencies, except the Department of Defense, to participate in the DHS CDM program. This means that the Coast Guard is not currently participating in the CDM program.

The DHS CIO’s decision has adversely affected the Department’s information security program in certain key areas, such as risk management, weakness remediation, system inventory, incidents reporting, and continuously monitoring. Specifically, the Coast Guard does not provide security metric data to be reported in DHS’ monthly information scorecard or participate in the Department’s CDM Program. Without Coast Guard’s security metric data or participation in DHS’ CDM program, the Department’s senior officials cannot consistently capture qualitative and quantitative performance measures or monitor security controls effectively. In addition, the CIO’s decision was not risk-based, as the Coast Guard has failed to meet the Department’s performance targets for security authorization and weakness remediation between fiscal years 2008 and 2019. Without justification, the Coast Guard has not reported its incidents to DHS since September 2012.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Housing and Urban Development

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	1	0
Protect	Managing Risk	Defined	E-mail	18	7	15
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	41	49	14
			Loss or Theft of Equipment	5	4	0
			Web	11	9	1
			Other	94	25	11
			Multiple Attack Vectors	4	1	1
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>173</b>	<b>96</b>	<b>42</b>

### CIO Self-Assessment

HUD's Office of the Chief Information Officer (OCIO) is excited to announce the successful initiation of the enterprise-wide Cyber Program. The Cyber Program will facilitate OCIO's mission and vision by integrating advanced cybersecurity technologies, processes, and policies to enhance HUD's ability to defend against evolving cyber threats and to drive innovation and transformation across the organization. HUD's Cyber Program seeks to:

- Build a comprehensive security program with enhanced technical capabilities to support HUD functional owners and protect high-value IT assets
- Implement the necessary governance processes to ensure compliance with Federal cybersecurity requirements and industry best-practices
- Create a culture of cybersecurity throughout HUD enterprise

To date, HUD has successfully completed a current state analysis of the cyber environment and mission-critical systems, existing vulnerabilities and risks, audit findings, and processes and policies that drive program operations. HUD is taking a phased approach to stand up the new Cyber Program. Some of the significant accomplishments include:

- Development of a cyber strategy and roadmap with defined goals and milestones
- Initial standup and operation of a 24/7 security operations center (SOC)
- Inventory of existing risks and audit findings/recommendations
- Centralized program management function to enable coordination across program offices and functional business units

HUD is focused on formalizing the Cyber Program, facilitating cyber awareness and innovation, and ultimately transforming

### Independent Assessment

The HUD information security (IS) program was evaluated as not effective. Long outstanding FISMA recommendations and ineffective or inconsistent processes throughout HUD program offices had prevented HUD's IS program from maturing. Significant limitations and challenges, such as constant senior leadership turn-over, had contributed to the lack of an effective IS program. HUD OIG did observe evidence of key efforts by the CIO and his staff in FY19 to address HUD's IS and Information Technology (IT) challenges. Continuity and proper oversight is essential for HUD to achieve an effective IS program.

The large number of legacy systems maintained by HUD continued to create challenges to the IS program, as they are resource-intensive and generally introduce risk to the computing environment. HUD's enterprise and IT risk management program, which is immature but continuing to slowly improve, severely hinders its ability to efficiently and effectively modernize its legacy systems and establish IS program priorities. In addition, HUD struggles with procurement challenges, effecting its ability to timely award IT contracts and provide proper oversight.

However, HUD began addressing critical issues that HUD OIG observed in previous years. The HUD OCIO began and had early successes in modernizing some of the HUD infrastructure, such as the data centers, some cloud adoption, and a mainframe system. The HUD CISO and Deputy CIO for Infrastructure and Operations was also filled in the last quarter of FY19; each being vacant for more than 2 years. Finally, the CIO initiated a tiger team to address and create remediation plans for open FISMA recommendations.

OIG recommends that HUD prioritize its IS program by assessing and maturing the FISMA domains and develop an IT strategic modernization roadmap to encourage a focused approach, continuity, and accountability.

HUD's cyber maturity over the next 12-month period. During the next phase, HUD OCIO will:

- Update the existing Authorizations to Operate (ATOs) to ensure systems-related security risks are consistent across the organization, reflect organizational risk tolerance, and align to HUD's Cyber Program goals
- Implement governance and risk management domains to enhance IT policies

# FY2019 Annual Cybersecurity Performance Summary

## Department of Justice

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	6	6	1
Protect	At Risk	Consistently Implemented	E-mail	339	610	378
Detect	Managing Risk	Consistently Implemented	External/Removable Media	1	0	1
Respond		Managed and Measurable	Impersonation	NA	1	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	513	175	199
			Loss or Theft of Equipment	1,267	42	14
			Web	61	82	9
			Other	457	270	184
			Multiple Attack Vectors	30	2	1
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2,674</b>	<b>1,188</b>	<b>787</b>

### CIO Self-Assessment

In FY 2019, the Department of Justice focused on modernizing IT, leveraging cloud services, and closing data centers for the purpose of enhancing our cybersecurity posture. While these measures improved data security, they also introduced new risks such as information storage outside of the traditional perimeter. To address these risks, the Department enhanced the architecture of the Justice Cloud Optimized Trust Internet Connection Services (JCOTS) to extend perimeter security protections to data stored within the cloud. In conjunction with the Justice Security Operations Center (JSOC), JCOTS prevented breaches by blocking malicious e-mails and identifying suspicious events for investigation. The JSOC and JCOTS' success led to OMB's designation of the Department being the Federal Security Operations Center as a Service provider. During the next fiscal year, DOJ will continue to assess emerging risks and adapt to the evolving threat landscape.

### Independent Assessment

During fiscal year 2019, the Department of Justice (Department) Office of the Inspector General (OIG) reviewed the information security programs of 6 Department components and a sample of 14 systems within these components. As a result of our review, the OIG determined that the maturity level for the Department's information security program is "Level 3 - Consistently Implemented" across four Security Functions: Identify, Protect, Detect, and Recover; and "Level 4 - Managed and Measurable" for the Security Function, Respond. Therefore, the OIG determined that one of the five Security Functions, Respond, is effective. However, the OIG determined that the Department's overall information security program is not effective due to the exceptions noted within the four Security Function areas of Identify, Protect, Detect, and Recover. 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, Incident Response, and Contingency Planning metrics of the Identify, Protect, Detect, Respond, and Recover Functions to improve the effectiveness of the Department's information security program.

# FY2019 Annual Cybersecurity Performance Summary

Department of Labor

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	1	2	1
Protect	Managing Risk	Managed and Measurable	E-mail	23	35	25
Detect	Managing Risk	Consistently Implemented	External/Removable Media	2	0	1
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	53	81	96
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	117	100	97
			Web	6	16	2
			Other	97	50	100
			Multiple Attack Vectors	6	0	0
			<b>Total</b>	<b>305</b>	<b>284</b>	<b>322</b>

## CIO Self-Assessment

In FY 2019, DOL continued its focus and enhancements in its cybersecurity program to include: Inventory of Systems & Assets, Security Incident Response, ISCM, Security Management, and Enterprise Information Technology initiatives.

Building on the prior year's successes, DOL further enhanced its Information Technology (IT) management and security capabilities by acquiring additional solutions and implementing previously acquired enterprise solutions that enhance the Department's IT asset management, provide automation and near real-time awareness of vulnerabilities

The Department continues its approach to strengthen the IT infrastructure with the integration and synergy of all DOL General Support Systems (GSS) into single DOL CDM Dashboard resulting in an enterprise, centralized risk monitoring capability across the Department. DOL implemented additional DHS CDM tools for vulnerability management resulting in lower enterprise wide costs via consolidated licensing and manpower versus a federated model. DOL will continue to emphasize a focus on strengthening its cybersecurity management functions.

These enhancements as well as those planned for the future will further prepare the Department to anticipate and mitigate risk and stay ahead of the evolving threat landscape.

## Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, DOL has consistently implemented its information security program and practices (policies, procedures, and tools) for the five cybersecurity functions and eight FISMA domains. We identified 23 deficiencies within all five cybersecurity functions and seven of the eight FISMA metric domains based on a selection of fifteen federal and five contractor information systems, and entity wide testing. Based on the maturity level calculation, it was determined that DOL's information security program was ineffective because only two cybersecurity metric domains were assessed at Managed and Measurable and the remaining functions and domains were assessed at the Consistently Implemented, which is how OMB, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency defined an effective program.

# FY2019 Annual Cybersecurity Performance Summary

## Department of State

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Defined	Attrition	8	36	10
Protect	Managing Risk	Defined	E-mail	2,598	3,082	1,043
Detect	Managing Risk	Ad Hoc	External/Removable Media	8	2	1
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	525	514	609
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	27	22	8
			Web	281	353	158
			Other	877	541	495
			Multiple Attack Vectors	81	10	52
			<b>Total</b>	<b>4,405</b>	<b>4,560</b>	<b>2,376</b>

### CIO Self-Assessment

The Department of State (DOS) is a target of interest for numerous threat actors. Evidence of this is observed at our network perimeter on a daily basis. To address this threat, DOS employs the Cyber Security Framework to which it aligns each improvement area. For FY 2019, in addition to completing system authorization assessments, the DOS continues the implementation of a new identity management system with the goal of a single identity for on-premise, remote access and cloud services. DOS also continues modernizing both legacy systems and remote access platforms to improve security protections.

For systems authorizations, DOS employs the risk management framework (RMF) to identify, assess, and respond to weaknesses identified. The RMF is applied following a ruleset that prioritizes high value assets (HVA) first followed by high, moderate and low impact systems. HVAs are also subjected to DHS assessments and expanded monitoring and penetration testing.

The FY 2019 Office of Inspector General Audit of the Department of State Information Security Program recommended implementation of an information risk management strategy. In response, DOS revised its previously approved cyber risk management strategy that now aligns directly with NIST SP800-39 and includes a high-level description of how the strategy is applied. Underway at this time is the development of a plan that oversees investment, acquisition and maintenance of IT assets whose decisions will be informed by cyber risk information. Additionally, DOS will complete the establishment of a new office of information risk to formalize FY 2018-19 investments in its information risk program.

There is no finish line to cybersecurity, and with this in mind, DOS is actively pursuing solutions to the risks arising from its reliance on IT. The efforts establish the programs and capabilities to improve its current state and prepare to counter new threats.

### Independent Assessment

Acting on behalf of the Office of Inspector General, an independent auditor, conducted this audit to determine the effectiveness of the Department's information security program and practices in accordance with FISMA requirements in FY 2019. The independent auditor concluded that the Department does not have an effective organization-wide information security program for several reasons. OIG made two recommendations to improve Department's information security program.

# FY2019 Annual Cybersecurity Performance Summary

## Department of State Office of Inspector General

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Optimized	Attrition	0	0	0
Protect	Managing Risk	Optimized	E-mail	0	0	0
Detect	Managing Risk	Optimized	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Optimized	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	3	0
			Web	0	0	0
			Other	0	1	0
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>4</b>	<b>0</b>

### CIO Self-Assessment

The Department of State Office of Inspector General (OIG) network supports its mission to conduct independent audits, inspections, evaluations, and investigations to promote economy and efficiency and to prevent and detect waste, fraud, abuse, and mismanagement in the programs and operations of the Department of State and the U.S. Agency for Global Media. OIG operates an independent network that is fully aligned with the Risk Management Framework and FISMA requirements. 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.

OIG took several actions in FY 2019 to mitigate cybersecurity risks and bolster defenses, including the completion of a DHS Risk and Vulnerability Assessment of OIG's general support system and major applications, a third-party FISMA assessment in support of renewing system authority to operate, and the implementation of additional endpoint and cloud security solutions. OIG received an overall rating of "Managing Risk" on the FY19 Q2 and Q4 Cybersecurity Risk Management Assessment.

- OIG established additional security and privacy policies to improve protection strategies and management of cybersecurity risks to the enterprise.
- OIG established additional dashboards to improve situational awareness concerning emerging cyber threats and vulnerabilities.
- OIG completed a SOC maturation plan and implemented a project plan to achieve target desired states of key cybersecurity capabilities and services.
- OIG enhanced its enterprise-wide phishing program and improved user resilience against top cybersecurity threats.

### Independent Assessment

Independent auditors conducted 2019 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, processes and technology) to support OIG mission. During interviews, demo, review of artifacts/evidence, the independent auditor 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 with 2018 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. 2019 IG FISMA Metrics audit reflected solid cybersecurity and risk management frameworks. We did identify areas of improvement through recommendations and recognized that although highest metric level may not be accomplished for a specific metric, OIG has implemented a comprehensive, defense-in-depth architecture to be effective and exceed OIG mission expectations.

# FY2019 Annual Cybersecurity Performance Summary

## Department of the Interior

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	2	0	2
Protect	At Risk	Managed and Measurable	E-mail	47	4	8
Detect	Managing Risk	Managed and Measurable	External/Removable Media	4	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	81	143	255
			Loss or Theft of Equipment	14	18	13
			Web	176	68	17
			Other	175	172	263
			Multiple Attack Vectors	12	2	2
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>511</b>	<b>407</b>	<b>560</b>

### CIO Self-Assessment

William E. Vajda became the new Department of the Interior (DOI) CIO in March 2019, filling a vacancy from September 2018. DOI updated internal policies to ensure internet-facing system vulnerabilities are resolved within the fifteen-day reporting and resolution requirement prescribed by DHS Binding Operational Directive (BOD) 19-02. DOI has engaged DHS technical services to examine Tier-1 High Value Assets (HVA) to comply with OMB M-19-03. DOI will start the required assessments of Tier2 and Tier 3 HVAs in FY20. Testing and training for social engineering continues to mitigate the scale of exploitation. DOI has made great strides to improve its enterprise level incident response capabilities in fiscal year 2019. DOI has improved its exfiltration protection and detection tools to limit privacy breach and data loss. DOI continues to respond to High Risk rated Risk Management Assessment (RMA) measures to include fully implementing the CDM Program and consolidating Security Operations functions into a single Enterprise Security Operations Center (SOC). DOI is looking forward to improved supply-chain risk management through OMB's implementation of Title 41 updates.

### Independent Assessment

A Performance Audit was performed over the information security program of the Department of the Interior (DOI) to determine the effectiveness of such program for the fiscal year ending September 30, 2019. 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 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 114 operational unclassified information systems and 11 information systems were randomly selected for the audit.

Consistent with applicable FISMA requirements, OMB policy, and NIST standards, DOI established and maintained its information security program and practices in the five cybersecurity functions, Identify, Protect, Detect, Respond, and Recover. However, the program was not effective as weaknesses were identified in three of the five function areas, Identify, Respond, and Recover. The Protect and Detect function areas were effective.

Weaknesses were noted in the FISMA domain areas of risk management, configuration management, data protection and privacy, incident response, and contingency planning metric domains. Consistent with the Fiscal Year (FY) 2019 OIG FISMA metric rating instructions, ratings throughout the eight FISMA domains were identified by a simple majority, where the most frequent level across the FISMA metrics served as the domain rating. The audit assessed the cybersecurity Protect and Detect functions at Managed and Measurable. The Identify, Respond and Recover functions were assessed at Consistently Implemented. Overall, DOI was assessed at Consistently Implemented.

# FY2019 Annual Cybersecurity Performance Summary

## Department of the Treasury

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	1	1	0
Protect	At Risk	Consistently Implemented	E-mail	10	5	54
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	1
Respond		Consistently Implemented	Impersonation	NA	1	6
Recover	At Risk	Consistently Implemented	Improper Usage	95	114	14
			Loss or Theft of Equipment	95	16	10
			Web	8	5	3
			Other	248	43	54
			Multiple Attack Vectors	2	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>459</b>	<b>185</b>	<b>142</b>

### CIO Self-Assessment

The mission of the Department of the Treasury is to maintain a strong economy and promote 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 sensitive financial and personal information affecting the transaction of trillions of dollars. Treasury faces cybersecurity risks inherent in its interactions with private and other public-sector organizations, limitations of authentication technologies, reliance on externally managed critical infrastructure, and current lack of centralized visibility of agency information technology assets and networks. The likelihood of risk realization is magnified by evolution in the volume, sophistication, and frequency of cyber threats. While Treasury leadership is engaged in the development of plans to address these risks, mitigation will require additional investments over the next several years to enhance capabilities and to recruit, maintain, and retain a capable workforce.

In FY 19, the Department continued to leverage investments from the Cybersecurity Enhancement Account (CEA) to mitigate cybersecurity risks. Some of these investments supported High Value Assets (HVAs). Treasury created enhanced risk profiles for all HVAs in FY 19 to provide leadership with greater visibility into associated risks, and with DHS completed RVAs and SARs of eight HVAs. Bureaus have already remediated most of the findings identified during these assessments. In addition, Treasury greatly improved its ability to combat spoofed email by increasing DMARC implementation to 98% of applicable domains. Treasury also made significant strides in the deployment of CDM tools, which are expected to provide greater awareness of our IT asset vulnerabilities beginning in FY 20.

### Independent Assessment

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 effective according to DHS criteria and as reflected in the deficiencies that the Independent Public Accounting (IPA) firm identified in Configuration Management, Identity and Access Management, Data Privacy and Protection, and Security Training. In addition, the IPA did not assess any of the FISMA Metric Domains as Managed and Measurable. The IPA assessed Treasury's Information Security program and practices for its unclassified systems as Consistently Implemented.

Consistent with applicable FISMA requirements, OMB and CNSS policy and guidance, and NIST standards and guidelines, Treasury established and maintained its information security program and practices for its Collateral NSSs for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program was not effective according to DHS criteria and as reflected by the deficiency that the IPA identified in the CM program area. In addition, the IPA did not assess any of the FISMA Metric Domains as Managed and Measurable; they were assessed as Consistently Implemented. The FY 2019 IG FISMA Reporting Metrics define an effective information security program as Managed and Measurable.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Transportation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	1	1	2
Protect	At Risk	Defined	E-mail	49	27	15
Detect	Managing Risk	Defined	External/Removable Media	3	0	1
Respond		Defined	Impersonation	NA	2	0
Recover	At Risk	Defined	Improper Usage	111	172	92
			Loss or Theft of Equipment	71	93	0
			Web	130	174	40
			Other	297	324	157
			Multiple Attack Vectors	11	10	4
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>673</b>	<b>803</b>	<b>311</b>

### CIO Self-Assessment

DOT continues to remediate identified weaknesses, reduce risks, and make improvements to its cybersecurity program. In FY 2019, DOT continued the support of integrated IT spending reviews for the operating administrations (OAs) subject to OCIO FITARA oversight; identifying potential duplication, misalignment, risks, and explicit gaps within OA cybersecurity programs and plans; and realigning and consolidating IT commodity resources and functions. As a outcome of these efforts, DOT maintained performance at an overall rating of "Managing Risk". The DOT CIO also invested in a new capability to assess and monitor the security of agency web sites which has significantly reduced common weaknesses and vulnerabilities and awarded an enterprise cybersecurity blanket purchase agreement that will support both the agency program and OA program needs. The continued IT commodity consolidation and network modernization initiatives have resulted in improved management of IT infrastructure, enhanced consistency in control implementation across the enterprise, and improved times to remediation for incidents and vulnerabilities.

### Independent Assessment

The information security program of DOT was evaluated as not effective. The independent auditor concluded that in all five function areas, DOT is at the Defined maturity level - the second lowest level in the maturity model for information security programs. The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT still faces challenges in the consistent implementation of its information security program across the Department. In addition, controls need to be applied in a holistic manner to information systems across DOT in order to be considered consistent and fully effective by achieving at least a rating of Managed and Measurable.

Consequently, the independent auditor noted weaknesses in each of the eight Inspector General FISMA Metric Domains encompassing the Departments Agency-wide program. The audit identified continuing deficiencies related to risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

# FY2019 Annual Cybersecurity Performance Summary

## Department of Veterans Affairs

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	1	3	0
Protect	Managing Risk	Defined	E-mail	614	358	162
Detect	Managing Risk	Defined	External/Removable Media	19	4	14
Respond		Managed and Measurable	Impersonation	NA	3	2
Recover	At Risk	Consistently Implemented	Improper Usage	107	75	13
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	394	362	498
			Web	723	239	89
			Other	773	732	49
			Multiple Attack Vectors	30	0	0
			<b>Total</b>	<b>2,661</b>	<b>1,776</b>	<b>827</b>

### CIO Self-Assessment

The VA operates a robust enterprise-wide RMF program that is fully aligned with NIST guidelines to include NIST Special Publications 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 Authorities to Operate (ATO) and any residual risk is monitored and managed via system-specific Plans of Actions and Milestones (POA&Ms). The Department's HVAs are identified 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, in alignment with the 2018 DHS Binding Operational Directive (BOD) 18-02, "Securing High Value Assets." Additionally, DHS assessed two VA HVA systems in the spring of 2019 to perform RVA and Security Architecture Review (SAR) reports. DHS conducted assessments on these two HVAs and VA is in the process of developing remediation plans to address the vulnerabilities identified during the assessment. Additionally, VA is in the process of establishing an HVA Program Office, in accordance with OMB M-19-03, "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program." The Program Office will enable the incorporation of HVA activities (e.g., assessment, remediation, incident response) into broader VA planning activities for information system security and privacy management, such as Enterprise Risk Management, Contract Management, and Contingency Planning. VA will be implementing the HVA Security Overlays, provided by DHS, that provide additional security controls to make HVAs more resistant to attacks, limit the damage from attacks when they occur and improve resilience. Additional activities are taking place through VA's Enterprise Cybersecurity Program (ECSP) to address previous assessment findings.

### Independent Assessment

VA has made strides and implemented comprehensive security controls in many areas including enhanced monitoring of network traffic, scanning and patching of devices, and standardization of security control functions. However, VA still faces many challenges when it comes to consistently applying effective controls to its entire inventory of systems. Many issues continue to be identified related to significant risk areas such as access and configuration management on some systems while others are receiving more attention/resources. Additionally, VA is not consistently or completely addressing all aspects of the RMF for its entire system portfolio. Due to the issues we identified throughout the audit cycle, we have assessed the VA's overall information security program to be ineffective.

# FY2019 Annual Cybersecurity Performance Summary

## Election Assistance Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	At Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

In FY 2019, the Election Assistance Commission (EAC) OCIO began work on a complete network modernization project, which was completed in November 2019. This project included replacing outdated systems, servers, and services, and gaining an increased level of control over the EAC network that was not previously available.

### Independent Assessment

EAC overall security program is effective. The overall assessment of the EAC information system program is "Level 3: Consistently Implemented." EAC's information system program could be improved by implementing controls to ensure the agency conducts a periodic physical inventory, utilizes Security Content Automation Protocol (SCAP) tools, ensures all IT specialists receive specialized security training and deploys DHS Einstein tools. In addition, EAC needs to develop a supply chain risk management strategy to meet the December 2019 deadline in the SECURE Technology Act of 2018.

# FY2019 Annual Cybersecurity Performance Summary

## Environmental Protection Agency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	1	0	0
Protect	At Risk	Consistently Implemented	E-mail	27	5	2
Detect	At Risk	Consistently Implemented	External/Removable Media	2	0	0
Respond		Consistently Implemented	Impersonation	NA	1	0
Recover	At Risk	Consistently Implemented	Improper Usage	34	41	102
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	31	63	33
			Web	126	14	0
			Other	121	41	63
			Multiple Attack Vectors	1	0	1
			<b>Total</b>	<b>343</b>	<b>165</b>	<b>201</b>

### CIO Self-Assessment

System level risks, including those to HVAs supporting mission essential functions, have been determined to be at acceptable levels, though there are many unknown risks. Major risk areas include: insufficient resources; insider threats; remote users; and exfiltration defenses; inadequate network capacity and architecture to support important security capabilities; legacy and emerging technologies; acquisitions processes, and sub-optimal staffing levels, skills, and organization.

EPA currently has significant gaps in cybersecurity capabilities, human resources, and supporting infrastructure. 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, tool maintenance, 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. The EPA's Acting Deputy Administrator, who has been designated as the Senior Accountable Official for Risk Management, regularly reviews the agency's cybersecurity status and progress.

### Independent Assessment

The EPA has an effective information security program for the following eight security functions and related domains defined within the FY 2019 IG FISMA Reporting Metrics:

- Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

Overall, we concluded that the EPA has processes to consistently implement its policies, procedures and strategies to meet the requirements of the cybersecurity functions and related domains outlined in the FY 2019 IG FISMA reporting metrics.

# FY2019 Annual Cybersecurity Performance Summary

## Equal Employment Opportunity Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	1	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	1	0
			Loss or Theft of Equipment	0	1	0
			Web	0	0	0
			Other	3	1	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>4</b>	<b>3</b>	<b>1</b>

### CIO Self-Assessment

In FY 2019, the EEOC hired its first stand-alone CISO, a critical position whose responsibilities were tasked to the Deputy CIO. The EEOC also continued to make substantial progress in modernizing its technology infrastructure and mitigating major risks. EEOC will achieve full deployment of PIV authentication upon the removal of legacy directory services from client devices, which will be completed during FY 2020. In preparation for full PIV authentication, the Agency deployed Enterprise Physical Access Control systems (ePACS) and Light Activation Kits to its Field Offices in FY 2019. The EEOC actively addressed vulnerabilities including Emergency Directive (ED) 19-01 to harden the organization's Domain Name Service (DNS) infrastructure, and the Agency continues to work with the DHS and third-party vendors to address the remaining items needed to achieve full BOD 18-01 compliance. The EEOC complied with BOD 18-02, designating one major information system as a high-value asset (HVA). The Agency is in the process of conducting a comprehensive security assessment with DHS to include additional compliance reviews of security control configurations against new HVA requirements. To further secure the Agency's information resources, the EEOC began implementing newly procured technologies, including security incident and event monitoring system capabilities, a malware-sandbox quarantine, safe e-mail link assessments, premier advanced threat protection for e-mails and the Agency's document repositories, and appliances to provide network access control and access control lists.

### Independent Assessment

Based on the results of our performance audit we concluded that EEOC's information security program is generally compliant with the FISMA legislation and applicable OMB guidance. We determined EEOC's information security program is effective and provides reasonable assurance of adequate security.

# FY2019 Annual Cybersecurity Performance Summary

## Export-Import Bank of the United States

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	2	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
			Web	1	0	0
			Other	6	0	1
			Multiple Attack Vectors	1	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>10</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

EXIM has taken numerous comprehensive steps to mitigate cybersecurity risks to the agency, and the improvement in scores from FY 2018 to FY 2019 are indicative of that effort. In FY 2019, 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 thorough security control assessments and attained ATOs for vital EXIM systems. Plans of Actions & Milestones (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; twice conducted Phishing Test Exercises; deployed a Security Information and Event Management (SIEM) system; established Risk Acceptances (RAs) with approval from the Enterprise Risk Committee (ERC); conducted Penetration Testing; and continued to regularly review and update agency and program level security policies and procedures. EXIM participated in the DHS Eagle Horizon for a national-level exercise; conducted an Incident Response Tabletop Exercise, a Privacy and Contingency Planning Tabletop Exercise, and a Continuity of Operations (COOP) / Disaster Recovery (DR) exercise on various systems. EXIM determined that the agency has no High Value Assets (HVAs) per DHS definition for national support. EXIM provided resources to improve its vulnerability management, internal auditing processes, System Development Life Cycle (SDLC), and updated and implemented an improved ISCM program. EXIM worked with FISMA and Federal Information System Controls Audit Manual (FISCAM) auditors to determine agency and program level weaknesses, then developed POA&Ms to track remediation.

### Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, EXIM has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA program areas. Although we noted deficiencies impacting specific questions within the RM, DP, ISCM, IR, and CP metric domains, we determined its information security program was effective as we evaluated the majority of the FY 2019 IG FISMA Reporting Metrics at the Managed and Measurable or high maturity levels.

# FY2019 Annual Cybersecurity Performance Summary

## Farm Credit Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	3	0	0
Detect	At Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Managed and Measurable	Improper Usage	0	1	0
			Loss or Theft of Equipment	10	5	15
			Web	0	0	0
			Other	13	2	0
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>26</b>	<b>8</b>	<b>15</b>

### CIO Self-Assessment

The Farm Credit Administration (FCA) continues to mature its cybersecurity Risk Management Program. 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. In FY 2019, several enhancements were made to the risk management application including adding the capability to map identified risks to NIST security controls. The FCA risk register is reviewed weekly by the CIO and the senior Office of Information Technology (OIT) staff. During these reviews, changes in risk factors are discussed. The CIO discusses high-priority concerns with senior FCA staff members and FCA Board Members, as appropriate. As a result of our Risk Management Program, FCA has initiated additional risk mitigations in several areas in FY 2019, such as implementing a more wholistic multi-factor-authentication regimen. FCA has also hired a dedicated privacy professional to ensure maximum implementation of privacy controls. To ensure the security of examination data, FCA conducts intrusion prevention, encrypts sensitive database columns, and ensures TLS-encrypted connections with 100% of our institutions. FCA also conducts mobile device management, including policy enforcement and remote wipe of lost devices.

### Independent Assessment

The Office of Inspector General performed an independent evaluation of the Farm Credit Administration's (FCA or Agency) information security program and determined FCA's information security program was effective.

FCA's information security program contains the following elements:

- information security policies and procedures,
- risk based approach to information security,
- implementation of risk-based security controls,
- corrective action for significant information security weaknesses,
- Change Control Board,
- standard baseline configurations,
- patch management process,
- vulnerability and security control assessments,
- identity and access management program,
- alerts for suspicious activity and devices,
- security training program,
- continuous monitoring,
- weekly security meetings,
- incident response program, and
- continuity of operations plan and tests.

However, the OIG made two recommendations to the Office of Information Technology to strengthen and improve the Agency's information security and privacy program related to updating the agency's information security policy and Information Security Continuous Monitoring strategy.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Communications Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Consistently Implemented	Attrition	0	8	0
Protect	At Risk	Consistently Implemented	E-mail	3	5	4
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	Managing Risk	Managed and Measurable	Improper Usage	3	2	1
			Loss or Theft of Equipment	29	11	8
			Web	5	5	20
			Other	77	16	12
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>117</b>	<b>47</b>	<b>45</b>

### CIO Self-Assessment

The FCC recognizes the following cybersecurity risks to the agency:

1. Security ATOs not completed for all organization operated systems.
2. Findings and Recommendations from IG's FY 2018 FISMA Evaluation.
3. "Critical" and "High" vulnerabilities not remediated within their stated timelines.
4. Lack of two-factor PIV credential for user authentication.

The FCC has taken the following steps to mitigate these risks:

1. FCC has developed a 3-year plan to get to 100% ATOs by the end of 2020.
2. FCC has developed and implemented corrective action plans for all findings from IG's FY 2018 FISMA Evaluation.
3. FCC has developed a plan to remediate "Critical" and "High" vulnerabilities by September 2020.
4. FCC is currently identifying the best solutions for multi-factor authentication.

### Independent Assessment

The FY 2019 FISMA evaluation included the Federal Communication Commission's (FCC) network (i.e., FCCNet) and the FCC's core financial management system. While the FCC made improvements to processes within its overall Information Security Program since the FY 2018 FISMA evaluation in the areas of risk management (i.e., authorizing information systems), and contingency planning (i.e., testing information system contingency plans), independent auditors and the FCC OIG determined that the FCC's overall program was ineffective in FY 2019. Specifically, we assessed the FCC's security processes related to the five NIST Cybersecurity Functions and determined that one function (Recover) was at a maturity Level 4, Managed and Measurable, two functions (Identify and Protect) were at a maturity Level 3, Consistently Implemented, and two functions (Detect and Respond) were at a maturity Level 2, Defined. Additionally, the independent auditor noted control weaknesses in six of the eight domain areas within the five functions. The independent auditor did not note any control weaknesses in the Security Training and Contingency Planning domains. 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.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Deposit Insurance Corporation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	14	1	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	1
Respond		Managed and Measurable	Impersonation	NA	1	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	144	101	77
			Loss or Theft of Equipment	31	0	0
			Web	6	4	0
			Other	33	8	2
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>228</b>	<b>115</b>	<b>80</b>

### 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 2019 include further development of key policies and procedures impacting essential security control areas (e.g., release of a new ICAM Program Strategy and supporting architecture). The FDIC is nearing completion of a new backup data center to help ensure that information technology (IT) systems and applications supporting mission-essential functions can be recovered within targeted timeframes. Additionally, the FDIC is investing in a comprehensive IT strategy to modernize IT infrastructure and legacy applications.

Recent assessments of FDIC cybersecurity controls identified the following areas warranting additional focus and resources: enterprise risk management, network firewalls, privileged account management, protection of sensitive information, security and privacy awareness training, and security control assessments.

### Independent Assessment

The information security program of FDIC was evaluated as not effective. The OIG audit determined that the FDIC's information security program was operating at a Maturity Level 3 (Consistently Implemented). The audit covered key components of the FDIC's information security program and selected controls pertaining to two general support systems, one major application, and one contractor service.

The FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. The FDIC also took or was working to take steps to strengthen its security program controls following the FISMA audit conducted in 2018. For example, the FDIC developed new or revised security policies and procedures in key security control areas; issued a new ICAM Program Strategy and supporting architecture; and made substantial progress towards completing a new backup data center to help ensure IT systems and applications supporting mission-essential functions can be recovered within targeted timeframes.

However, the audit identified security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of information systems and data at risk. The highest risk weaknesses were in the areas of risk management, network firewalls, privileged account management, data protection and privacy, security and privacy awareness training, and security control assessments. The audit resulted in three new recommendations intended to ensure employees and contractor personnel properly safeguard sensitive electronic and hardcopy information and network users complete required security and privacy awareness training. The FDIC concurred with all three recommendations and planned to complete corrective actions by May 2020. The FDIC was also working to address an additional six recommendations from prior FISMA audit reports.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Energy Regulatory Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Optimized	Attrition	0	0	0
Protect	Managing Risk	Optimized	E-mail	0	0	0
Detect	At Risk	Optimized	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	1	0
			Other	5	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>5</b>	<b>1</b>	<b>0</b>

### CIO Self-Assessment

In FY 2019, FERC continued to make significant investment in maintaining, evolving and maturing a risk-based and cost effective cybersecurity program. Some highlights include: 1) Began implementing a robust Data Loss Prevention (DLP) solution to monitor and prevent sensitive data exfiltration; 2) Implemented a phishing reporting and analysis tool for proactive phishing protection capabilities; 3) Established enterprise-wide system risk thresholds and implemented trend analysis reporting for risk-based, cost-effective decision making; 4) Implemented Microsoft Azure Information Protection (AIP) to simplify the data labeling process for Controlled Unclassified Information (CUI). FERC continues to make progress towards meeting FY 2019 government-wide targets in the Cybersecurity CAP Goal metrics. Efforts to continue improving cybersecurity enhance the Commission's cybersecurity posture and support compliance with FISMA, as indicated in this year's report.

### Independent Assessment

Overall, the Office of Inspector General determined that the Commission had an effective information technology cybersecurity environment. In particular we found that the Commission consistently implemented (level 3) controls related to the Recover function. Additionally, we determined that the Commission achieved managed and measurable (level 4) performance related to the Protect function. We also concluded that the Commission met the optimized (level 5) maturity level for the Identify, Detect, and Respond functions.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Housing Finance Agency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	1
			Loss or Theft of Equipment	9	26	13
			Web	0	0	0
			Other	15	0	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>24</b>	<b>26</b>	<b>15</b>

### CIO Self-Assessment

FHFA continues to make progress toward meeting Cybersecurity CAP Goal metrics. By the end of FY 2019, FHFA met all CAP Goal metrics except for Automated Access Management. FHFA does not currently employ a dynamic access management solution. During FY 2019, FHFA reported a total of 18 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 Office of Inspector General's independent review, FHFA determined with reasonable assurance that as of September 30, 2019, FHFA's information security and privacy policies, procedures, and practices are adequate and effective.

### Independent Assessment

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 2019 IG FISMA Reporting Metrics. The IPA's methodology included testing the effectiveness of selected security controls implemented in a subset of systems in accordance with the NIST Special Publication (SP) 800-53, Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and Organizations. The IPA determined that FHFA implemented an effective information security program and practices and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall Managed and Measurable maturity level. Although FHFA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, the IPA noted weaknesses in two of the eight domains in the FY 2019 IG FISMA Reporting Metrics. As a result, the IPA made six recommendations to assist FHFA in strengthening its information security program.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Labor Relations Authority

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	1	0	0
			Web	0	0	0
			Other	0	0	1
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>1</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

The Federal Labor Relations Authority successfully navigated FY 2019 with no reported Cybersecurity incidents. The Authority was able to achieve a Domain-based Message Authentication, Reporting & Conformance (DMARC) policy of reject as directed by BOD 18-01. FLRA also closed many FISMA audit findings of the previous year and no new major findings were reported by the auditor. the Authority's users continue to reach out with cybersecurity questions, forward us suspicious email, and report possible cybersecurity incidents. As an agency we continue to provide users with ongoing education and to encourage them to take an active part to ensure the agency maintains a positive information security stature.

### Independent Assessment

The information security program of FLRA was evaluated as effective. FLRA has various controls in place such as access, audit, logical and physical, where those controls are pervasive throughout the agency. The scope of this year's FISMA audit can be found on the accompanying report.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Maritime Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	2	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	1	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>3</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The FMC has performed bi-annual risk assessments as defined by NIST to identify, estimate, and prioritize cybersecurity risk to the agency operations, assets, staff, and the public. We have identified the agency's critical information systems assets and determined the impact on the agency in the event of a cyber-attack or security incident. To protect the Commission's information technology assets, the agency has deployed security standards in response to DHS' Binding Operations Directives and continues to reduce internal and external vulnerabilities through the implementation of the CDM program cybersecurity tools and services.

### Independent Assessment

The overall IG assessment rating is "effective" for the Federal Maritime Commission (FMC). In the IG's fiscal year 2019 FISMA audit, the OIG identified three weaknesses, and also concluded the FMC had effectively implemented all of the prior year recommendations. FMC is a small, independent federal agency. As such, in some instances, the FMC does not have the resources, or in some cases the need, to implement the extent of controls at a greater level.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Mediation and Conciliation Service

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	High Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Managed and Measurable	Improper Usage	0	0	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	2
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>2</b>

### CIO Self-Assessment

FMCS has followed its cyber-security framework action plan and has secured the services of several contractors who have performed cyber-security 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 2020. This will allow FMCS to respond in a comprehensive manner to any incidents identified by the MSSP. FMCS has identified and submitted High Value Assets per BOD 18-02 and integrated them into the FMCS cyber security framework. By performing these actions, FMCS has made significant progress towards achieving level 4 maturity for these metrics.

### Independent Assessment

The information security program of FMCS was evaluated as effective. FMCS has followed its cyber-security framework action plan and has secured the services of several contractors to perform comprehensive cyber-security assessments to include suggested paths to successfully remediate any actions identified. FMCS procured software that will perform automated inventory of software, hardware and provide alerts of any software changes or remediation needs to system administrators. We plan to replace any deficient processes with automated services where possible in FY 2020 and beyond. By performing these actions, FMCS will make significant progress towards achieving level 4 maturity for these metrics.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Mine Safety and Health Review Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Managed and Measurable	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	2	0	1
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>2</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

To address ongoing and evolving cybersecurity risks, The Federal Mine Safety and Health Review Commission, herein the (Commission) have deployed and have in-progress information security compliance initiatives as mandated and in compliance with BOD 18-01. The Commission's cybersecurity risk abatement initiatives range from deployed to in-progress, targeting Q4 FY 2020 for completion of BOD 18-01 specific cybersecurity risk abatement efforts.

### Independent Assessment

The information security program of the Federal Mine Safety and Health Review Commission was evaluated as effective. FMSHRC deployed and has in-progress information security compliance projects to address information security concerns. End-Point Protection is deployed through the network infrastructure providing antivirus, data exfiltration, application control, email malware and phishing abatement. Network Access Control (NAC) and Network Access Protection (NAP) are implemented as a solution to detect and alert on the connection of an unauthorized hardware assets.

# FY2019 Annual Cybersecurity Performance Summary

## Federal Retirement Thrift Investment Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	15	12	4
			Loss or Theft of Equipment	13	18	13
			Web	1	0	0
			Other	75	2	5
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>104</b>	<b>32</b>	<b>22</b>

### CIO Self-Assessment

In FY 2019, the Federal Retirement Thrift Investment Board (FRTIB, or “the agency”) developed risk treatment plans for information security and disaster recovery risks. FRTIB created initiatives to address the risks for Information Security through its FISMA maturity roadmap and was able to achieve Level 3 (“Consistently Implemented”) maturity in four of eight FISMA domains. Disaster Recovery risks were addressed through table top exercises, the establishment of failover capabilities for critical business applications, the implementation of cloud-based email/storage, and additional storage at a secondary data center.

The Agency has made additional progress on the implementation of the government-wide CAP goals. Of the ten Cross Agency Priority (CAP) Goals for FY 2019, the agency has achieved all but one; Software Asset Management. The Agency is in the process of rolling out its implementation of Application Whitelisting and is on track to complete the implementation in Q2 of FY 2020. 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 2020 and beyond, with the goal of improving the Agency’s maturity across all FISMA domains.

### Independent Assessment

The information security program of Federal Retirement Thrift Investment Board was evaluated as not effective. FRTIB made improvements to its overall information security posture during FY 2019 by implementing control activities defined in the prior year and developing strategic and governing documents for the domains rated Ad-Hoc in previous years, with the exception of the contingency planning domain.

Although FRTIB made improvements to its information security program, the independent auditor identified recurring issues which prevent the agency from establishing an effective organization-wide program to identify, protect, detect, respond, and recover from information security weaknesses using a risk-based approach.

To reach this conclusion, the independent auditor assessed FRTIB’s information security program and related practices across the eight FISMA domains. Specifically, the independent auditor reviewed a combination of entity-wide and system specific controls with a particular focus on three of FRTIB’s information systems: Business Process Services (BPS), Core Recordkeeping Services (CRS), and Interfacing Services System (ISS).

# FY2019 Annual Cybersecurity Performance Summary

## Federal Trade Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	1	0
Protect	Managing Risk	Managed and Measurable	E-mail	6	3	1
Detect	At Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	8	18	7
			Loss or Theft of Equipment	0	0	2
			Web	1	0	0
			Other	6	1	0
			Multiple Attack Vectors	2	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>23</b>	<b>23</b>	<b>10</b>

### CIO Self-Assessment

The Federal Trade Commission (FTC) continues to manage Mission Essential Functions (MEF) risk by leveraging FedRAMP cloud service providers (CSP), such as cloud identity management and IT service management. The Agency continues to make progress converting legacy IT to modern cloud service offerings, but still relies on legacy IT for its on-premise data centers. Examples of progress include preventing the use of untrusted removable media, expansion of Network Access Controls, and adoption of E3 email security services. The CIO Ratings highlight the impact of accepted risks with remaining legacy IT that limits FTC's ability to fully implement technical capabilities while undergoing IT modernization. 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 limited bandwidth. To do so effectively, the Agency will exercise discretion over its authorization process through changes in policy to cost-effectively manage FISMA compliance.

### Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, FTC's information security program and practices were established and maintained for the five Cybersecurity Functions and eight FISMA Metric Domains. The overall maturity level of FTC's information security program was determined as Managed and Measurable, as described in the FY 2019 overall IG Assessment. Accordingly, we found that FTC's information security program and practices were effective for the period October 1, 2018, to September 30, 2019.

# FY2019 Annual Cybersecurity Performance Summary

## General Services Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	1	1
Protect	Managing Risk	Managed and Measurable	E-mail	78	5	4
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	44	49	65
			Loss or Theft of Equipment	230	0	0
			Web	6	3	2
			Other	76	21	24
			Multiple Attack Vectors	1	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>435</b>	<b>79</b>	<b>96</b>

### CIO Self-Assessment

In FY 2019, GSA took deliberate action to address cybersecurity risks to the agency. GSA further secured its highly mobile workforce by implementing a cybersecurity solution that provides visibility across all Internet connected mobile devices anywhere in the world, and to help stop phishing, malware, and ransomware earlier in the cyber kill chain by blocking DNS requests for malicious domains. The solution provides like protection to GSA endpoints that are not connected to the GSA network directly or via Virtual Private Network (VPN). GSA strengthened its DNS infrastructure by extending it to the cloud to achieve rapid elasticity, allowing DNS infrastructure to dynamically grow or shrink adapting to DDOS attacks; and, implemented BIND rate-limiting on every DNS server. The project has significantly improved GSA attack resistance to DDoS attacks and improved DNS availability.

GSA continues to meet or exceed all FY 19 CAP Goal targets; made significant progress in implementing all but one Risk Management Assessment (RMA) metric; and closed out residual High Value Asset (HVA) metric gaps, effectively meeting all HVA metrics.

To better secure GSA Privileged Users with network accounts against cyber attack, GSA implemented a technical solution for limiting all privileged account access from servers and workstations to trusted sites allowing GSA to achieve 100% compliance with the metric. Limiting privileged users access to trusted sites increases GSAs security posture by limiting risk to our most sensitive accounts and servers. Further, GSA implemented machine based two-factor PIV authentication for MAC workstations, significantly improving our performance from 0% to 72% in FY19 and plans to achieve the target goal of 95% for this metric in FY20.

GSA currently meets all HVA metrics for all of its HVA systems. GSA will ensure that HVA requirements are met for any new HVA systems added to the inventory in FY20.

### Independent Assessment

Consistent with applicable FISMA 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 domains. We identified three deficiencies within three of the five cybersecurity functions and three of the eight FISMA metric domains based on a selection of eight information systems (six GSA information systems and two contractor information systems) and entity wide testing. GSA closed five of 10 prior year recommendations and the remaining five are open. Based on the maturity level that CyberScope calculates, it was determined that GSA's information security program is not effective because four cybersecurity functions were assessed at Managed and Measurable and the remaining one was assessed at Consistently Implemented, which is how OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency defined an effective program.

# FY2019 Annual Cybersecurity Performance Summary

## Gulf Coast Ecosystem Restoration Council

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### 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 NIST Risk Management Framework. The Council's IT systems are protected according to Federal and Industry best practices to ensure confidentiality, integrity, and availability. Actions taken by the Council include leveraging security contracts to protect IT assets and implementing required Federal services such as continuous diagnostics and monitoring services. These services allow the Council to ensure the identification and protection of assets and then detect, respond, and recover from cyber incidents. Overall the Council's information assurance program is effective and meeting the targeted security goals.

### Independent Assessment

In its report, an independent certified public accounting firm concluded that 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 eight FISMA Metric Domains. The independent assessor found that the Council's information security program and practices were effective. The overall maturity level of the Council's information security program was determined as Managed and Measurable based upon a simple majority of the maturity level for each of the domains, and due to the CIO's direct involvement in every IT security decision, direct oversight of security controls, and the simple IT structure of stand-alone computers and service vendors. Our tests of effectiveness found no exceptions.

# FY2019 Annual Cybersecurity Performance Summary

## Institute of Museum and Library Services

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond	At Risk	Managed and Measurable	Impersonation	NA	0	0
Recover		Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

Major focus areas for the Institute of Museum and Library Services (IMLS) in FY19 were to significantly strengthen its overall security posture by mitigating key risks identified in enterprise-wide IT assessment that IMLS undertook in FY2018 and migrate IMLS applications/network components to interagency shared services and FEDRAMP compliant cloud-based services utilizing IaaS and SaaS models.

IMLS successfully adopted Shared/Cloud based services for most of its mission critical applications/network components, which led to better security management by leveraging automation, patch management, and monitoring capabilities provided by the Cloud Service Provider, as well as higher availability and optimal values for recovery parameters in case of a disaster.

During FY2019, IMLS achieved 100% compliance in Credentialing and Authorization domain by requiring IMLS staff to use PIV and/or dual factor authentication to access its information resources. More robust centralized asset management tools were deployed to better monitor, track, and report Software/Hardware inventory. IMLS has enhanced its Audit and Accountability security controls by employing an enterprise wide log management tool to receive real-time alerts when an unusual activity on network is encountered and to efficiently monitor, report, and audit its network. IMLS implemented auto-detection and prevention of any unauthorized removable media connected to IMLS provided laptops. A similar mechanism to prevent rouge devices introduced into the network is currently in evaluation phase and scheduled to be fully operational by December 2019.

Comprehensive System Security Plans were developed for two mission critical systems. Authority to Operate has been issued upon successful remediation of all medium/high priority deficiencies identified in the system assessment.

An independent third-party audit of the IMLS environment was performed in Q4 FY2019. It was determined that the IMLS information security program was effective.

### Independent Assessment

The scope of this audit covers the IMLS GSS. An independent auditor performed an assessment of the effectiveness and level of implementation for ISCM, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other supporting documentation as it pertains to the IMLS GSS. The IMLS information security program was found to be implemented effective 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;
- ISCM processes are well established by assigning ISCM activities to IMLS stakeholders with defined frequencies and security requirements;
- Vulnerability scanning of agency information systems and assets has been established and is performed according to FISMA security requirements and frequencies;
- IMLS has established an effective configuration management program for its information systems by employing the use of automated mechanisms that provide on demand and real-time baseline, security configuration requirements, and risks views of the entire agency infrastructure;
- Automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, ISCM, and Configuration Management programs;
- IMLS ensures that Security training is monitored and provided to IMLS stakeholders at least annually and given to IMLS personnel according job functions and levels of access;
- IMLS has established and maintained an effective Incident Response program that includes validated processes for responding, containing, and reporting security incidents to oversight agencies.

In November 2019, IMLS conducted a table top exercise of its contingency plan and document lessons learned.

#### Next Steps:

- Implement an automated mechanism to prevent saving PII to local devices;

# FY2019 Annual Cybersecurity Performance Summary

## Inter-American Foundation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	1
Protect	At Risk	Consistently Implemented	E-mail	0	0	0
Detect	At Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

Inter-American Foundation (IAF) is a small government corporation that over the past five years has invested in its information technology (IT) program to comply with all Federal mandates and recommendations to the best of its abilities. As part of the annual OIG FISMA audit, it was concluded that the Inter-American Foundation (IAF) generally complied with FISMA by implementing 78 of 89 security controls reviewed for selected information systems.

IAF effectively:

- Improved documentation of its risk management policy, procedures, and strategy;
- Established an organization structure to improve the process for reviewing, approving and documenting configuration management changes;
- Conducted table-top exercise to test its Continuity of Operations Plan (COOP) to ensure the availability and effectiveness of the plan; and
- Updated the Foundation's standard operation procedures.

IAF systems does not work with any classified information and limited sensitive and PII information. IAF had no data breach and systems were available 99.99% of the time.

Our financial and HR systems including payroll are outsourced to other shared service providers.

IAF over time has improved its security posture and it will continue to utilize all resources to continue that mission and improve efficiency as well and IAF has a plan to mitigate the FISMA findings in next six months that were identified in the audit of FY19.

### Independent Assessment

Overall, the Inter-American Foundation (IAF) is at level 3. Their consistent implementation on IG's maturity model spectrum was rated as not effective. Based on the result of tests performed on 89 security controls over selected IAF systems, the independent assessor determined that IAF's information security program to protect the confidentiality, integrity, and availability of its information and information systems was effective. The independent assessor noted that 78 of the 89 Security Controls (88 percent) were designed suitably and operating effectively. Based on our analysis, improvements are needed in the following NIST Cybersecurity function areas:

1. Identity - Risk Management
2. Protect - Security Training
3. Protect - ICAM
4. Recover - Contingency Planning

# FY2019 Annual Cybersecurity Performance Summary

## International Boundary and Water Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	1	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>1</b>	<b>0</b>

### CIO Self-Assessment

The United States International Boundary and Water Commission (USIBWC) consist of one Moderate Security Level General Support System (GSS) and two High Security Level 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 OMB and NIST. The USIBWC is in the process of reauthorizing a security assessment and authorization for its GSS and SCADA systems for the International Wastewater Treatment Plants in Nogales, AZ and San Ysidro, CA. The agency anticipates a renewed GSS and SCADA Authority to Operate (ATO) designations to be issued in FY 2020. The USIBWC is in the process of developing and implementing an ongoing ISCM Program for all three Systems. The USIBWC is leveraging procurement resources for necessary CDM services and anticipates award and implementation of CDM services to be in place in early 2020.

### Independent Assessment

The information security program of the USIBWC was evaluated as effective. OIG found that USIBWC generally implemented an effective information security program that supported its operations and assets, despite limited staff and resources being dedicated to the relocation of its headquarters. However, OIG noted deficiencies that require remediation for USIBWC to fully comply with FISMA. OIG identified issues related to the risk management, ISCM, and contingency plan domains. OIG made four recommendations to help USIBWC improve their information security program.

# FY2019 Annual Cybersecurity Performance Summary

## International Trade Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	1
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	1	1
			Loss or Theft of Equipment	0	1	0
			Web	0	0	0
			Other	3	2	4
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>3</b>	<b>4</b>	<b>6</b>

### CIO Self-Assessment

The U.S. International Trade Commission (USITC) recognizes it must continually improve the adequacy and effectiveness of its cybersecurity and privacy policies, procedures, and practices. For FY 2019, USITC has either met or exceeded the target for eight of the nine applicable CAP goals. USITC does not have HVAs, and as a result, CAP goal A6. HVA System Access Management does not apply. USITC has made significant progress towards meeting CAP goal A1. SWAM. The Commission continues to update and modernize its IT systems to meet evolving threats and emerging business requirements. The Commission workstation operating system has been upgraded to Microsoft Windows 10 and Fifty-seven percent of our Linux environment has been updated to Red Hat Enterprise Linux version 7.

### Independent Assessment

The information security program of U.S. International Trade Commission was evaluated as effective. USITC enforces application control across all compatible devices for user's desktop and laptop devices, demonstrating 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, demonstrating that the Commission has effective patching of software on its network. The Commission has a successful security and awareness program, which trains all users on how to identify current cyber security threats and how they are to be handled.

# FY2019 Annual Cybersecurity Performance Summary

## Japan-United States Friendship Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The cybersecurity risks have not changed for the Japan-US Friendship Commission (JUSFC) since the last reporting period. The JUSFC continues to use industry standard and US government approved systems to protect our assets.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the JUSFC was not performed for FY 2019 and the IG assessment section was marked "Not Applicable." 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 JUSFC will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Marine Mammal Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Optimized	Attrition	0	0	0
Protect	At Risk	Optimized	E-mail	0	0	0
Detect	Managing Risk	Optimized	External/Removable Media	0	0	0
Respond		Optimized	Impersonation	NA	0	0
Recover	Managing Risk	Optimized	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The Marine Mammal Commission (MMC) 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 MMC's office is located in Bethesda, Maryland. The MMC does not own or manage any information systems. Any PII is collected only for necessary purposes and is secured. The main means of ensuring security of federal information are as follows:

- 1) The MMC does not originate, receive, or store classified information, either electronically or in hard-copy. The MMC has a suitably rated safe that is kept in a locked room for storing such information, if the need should arise.
- 2) The MMC's official personnel records are maintained by the GSA, 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 MTIPS to provide a TIC. The MMC has signed the EINSTEIN Memorandum of Agreement with the DHS.
- 4) All agency computers have antivirus software installed.

### Independent Assessment

The information security program of the Marine Mammal Commission was evaluated as effective. MMC is a micro-agency consisting of three Commissioners and nine members of the Committee of Scientific Advisors on Marine Mammals, all of whom are special government employees, supported by a staff of 14 full-time government employees. The MMC's office is located in Bethesda, Maryland. The MMC does not own or manage any information systems. Any PII is collected only for necessary purposes and is secured. The main means of ensuring security of federal information are as follows:

- 1) The MMC does not originate, receive, or store classified information, either electronically or in hard-copy. The MMC has a suitably rated safe that is kept in a locked room for storing such information, if the need should arise.
- 2) The MMC's official personnel records are maintained by the GSA, 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 MTIPS to provide a TIC. The Commission has signed the EINSTEIN Memorandum of Agreement with the DHS.
- 4) All agency computers have antivirus software installed.

# FY2019 Annual Cybersecurity Performance Summary

## Merit Systems Protection Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	0	0	1
Detect	At Risk	Defined	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	3	8	3
			Loss or Theft of Equipment	2	2	1
			Web	1	0	1
			Other	2	0	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>8</b>	<b>10</b>	<b>7</b>

### CIO Self-Assessment

The Merit Systems Protection Board (MSPB) deployed CDM in Q3 of 2019 and is now actively showing data on the DHS CDM dashboard. CDM enhanced MSPB's vulnerability and asset management as well as centralized the data.

MSPB implemented two-factor authentication for its office suite, and security policies for safe hyperlinks and anti-phishing in FY 2019. MSPB plans to add safe attachments policies in FY 2020.

MSPB has maintained existing TA, MEF, IPSS and DNS sinkhole protections through MTIPS. MSPB staff provided additional internal network and DMZ monitoring as well as a separate firewall below the MTIPS connection.

MSPB is currently working to modernize its legacy core business applications. A contract with a FedRAMP certified vendor is in place and the new system is on schedule to be in production in FY 2021.

### Independent Assessment

The information security program of MSPB was evaluated as not effective. An independent auditor examined the MSPB GSS. They assessed the effectiveness and level of implementation of ISCM, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other supporting documentation. 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 their GSS environment. In the auditor'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. 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 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 PII that is collected, used, maintained, shared, and disposed of by its information systems.

# FY2019 Annual Cybersecurity Performance Summary

## Millennium Challenge Corporation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	1	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	2
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	15	0	1
			Web	2	1	0
			Other	9	0	2
			Multiple Attack Vectors	0	0	1
			<b>Total</b>	<b>26</b>	<b>2</b>	<b>6</b>

### CIO Self-Assessment

Millennium Challenge Corporation (MCC) has complied with the goals of email security in BOD 18-01 and continues to leverage the President's Management Agenda of IT Modernization for migrating non-compliant systems to a modern, cloud-hosted SaaS to meet the web security portion of BOD 18-01. Contingency planning for the MCC needs to account for specific roles and responsibilities associated with IT contingency positions and the MCC needs to align IT restoration priorities with the latest changes to the BIA. Lastly, MCC allows for split tunneling, but mitigates this risk with application white-listing, and increasing log monitoring at the end points with Microsoft system monitoring service. Removing split tunneling impacts performance in remote foreign locations and negatively impacts the business requirements.

### Independent Assessment

The information security program of MCC was evaluated as effective. MCC's information security program was evaluated as part of the FY 2019 FISMA Audit. This audit included an evaluation of four out of seven FISMA reportable systems at MCC. The audit determined that 85 of the 101 instances of the selected NIST 800-53 security controls were properly implemented.

# FY2019 Annual Cybersecurity Performance Summary

Morris K. Udall Foundation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	High Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

## CIO Self-Assessment

In 2019, Morris K. Udall Foundation (UDALL) maintained the cybersecurity standards established in previous years. DHS continues to provide UDALL with weekly scan results relating to Cyber Hygiene, HTTPS, Trustworthy Email. UDALL opened a new dialog with DHS regarding their CDM program and anticipates approval in the upcoming fiscal year. Deficiencies such as software and hardware asset management will be addressed upon approval. To date, purchasing and implementing these systems have been both cost and time prohibitive. Security policies were drafted in FY19 and should be adopted into IT practice in FY20. UDALL continues to take steps to comply with BOD 18-01. In our most recent DHS scan UDALL scored 90% and is working with outside vendors to get the remaining items resolved. While 2FA using our PIV cards was a goal in 2019, it was delayed until 2020. However, PIV cards will not be involved in moving to 2FA. Other 2020 security goals are to improve our antivirus, malware threat and protection, and asset management and monitoring.

## Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Morris K. Udall Foundation (UDALL) was not performed for FY 2019, and the IG assessment section is marked "Not Applicable." 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 UDALL will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## National Aeronautics and Space Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	7	2	1
Protect	Managing Risk	Defined	E-mail	646	5	7
Detect	Managing Risk	Defined	External/Removable Media	3	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	209	180	1,329
			Loss or Theft of Equipment	249	23	15
			Web	354	30	3
			Other	333	76	108
			Multiple Attack Vectors	46	1	6
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>1,847</b>	<b>317</b>	<b>1,469</b>

### 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 it 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 (Corporate deployment has been completed), with Mission deployment continuing to rapidly improve each quarter. Additionally, NASA achieved a new Cyber CAP goal by ensuring 100% of Agency assets are scanned for malware prior to allowing remote network access, further solidifying NASA's ability to detect and prevent network intrusions. The Agency has also achieved 90% Personal Identity Verification (PIV) card authentication for unprivileged users and 100% for privileged users and is developing PIV solutions for various NASA systems, including MacOS, Linux, and Unix systems. Additionally, HVA inventorying and management continues to gain accuracy and improvement with NASA reaching a new HVA Risk Management Assessment (RMA) goal in FY 2019: encryption of HVA systems at rest. Together, CDM tools, increased PIV coverage, improved HVA management, and malware scanning coverage for remote access has continued to enable NASA to secure the Agency's network and resources in FY 2019.

### Independent Assessment

During the FY 2019 evaluation, NASA's information security policies, procedures, and practices were assessed by examining six (6) of the Agency's information systems. In addition, we assessed the Agency's overall cybersecurity posture utilizing a variety of processes, procedures, and techniques that leveraged prior work performed by NASA, NASA OIG, and GAO. In addition, we also evaluated NASA's progress in addressing deficiencies identified in prior FISMA evaluations and audits performed by the NASA OIG. Cumulatively, the results of these assessments assisted us in reaching our conclusions. By implementing previous audit recommendations and implementing corrective actions, NASA continues well on its path to improving its overall cybersecurity posture. However, as indicated by the results of this evaluation, information security continues to remain a significant challenge for NASA in addressing cybersecurity gaps in its efforts to address and counter cyber threats in an ever-evolving threat landscape. While NASA does continue to make progress in securing its networks and information systems, its cybersecurity program remains ineffective when judged using OMB's model, which requires agencies to achieve a managed and measurable maturity to be considered effective. In the five functional areas reviewed during this evaluation, NASA information systems remain vulnerable to cybersecurity threats.

# FY2019 Annual Cybersecurity Performance Summary

## National Archives and Records Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	2	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	2	0
			Loss or Theft of Equipment	0	0	0
			Web	6	2	3
			Other	71	4	7
			Multiple Attack Vectors	1	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>80</b>	<b>8</b>	<b>10</b>

### CIO Self-Assessment

IT security is a challenge for the National Archives and Records Administration (NARA). NARA information security policies, procedures, and practices provide adequate protections that are generally effective. However, in some cases NARA lacks the formal documentation necessary to ensure that its policies and strategies are consistently implemented. Because of long standing risks in NARA's IT security, IT security was declared a material weakness in internal controls from FY 2015 - 2019. NARA continues to improve its ability to protect the confidentiality, integrity, and availability of NARA resources. In FY 2019, NARA acquired a new contract which provided dedicated Information ISSO resources to information systems. NARA made significant progress toward the authorization of seven additional moderate impact systems. We expect these systems to be assessed and authorized in FY 2020 and expect to achieve authorization for 100% of our FISMA reportable systems in FY 2021. NARA also recently awarded a contract to implement a DHS tool to enforce 2FA using PIV cards for users with elevated security responsibilities. Additionally, NARA is taking steps to address email services in order to address the enhanced email security requirements of BOD 18-01. NARA plans to achieve 100% compliance with the BOD 18-01 email security requirements in FY 2020.

### Independent Assessment

The information security program of NARA was evaluated as not effective. NARA continues to stress their commitment to improving information security throughout the agency and is making steady progress to that end. NARA also continues to work to address open OIG audit recommendations related to its information security program. NARA made several noteworthy improvements during FY 2019 throughout the domain areas, which have been recognized in the IG metric responses as relevant and applicable:

- Through the addition of ISSO, NARA's development and maintenance of system security documentation generally improved.
- NARA broadened its identification of risks by improving its RMF Dashboard to incorporate more systems.
- NARA improved its system inventory reporting.

To fully progress towards consistently implemented, NARA needs to improve its identity and access management capability by:

- 1) developing and implementing an ICAM strategy;
- 2) ensuring privileged account reviews are conducted; and
- 3) ensuring the completion of system E-authentication risk assessments.

In addition, NARA also needs to provide better management oversight and follow up to ensure training is completed and documented by required individuals in a timely manner. NARA should improve its contingency planning function to ensure it completes and tests its system-level contingency plans, conducts system BIAs, and establish contingency planning strategies for cloud systems.

# FY2019 Annual Cybersecurity Performance Summary

## National Capital Planning Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	2	0	2
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	Managing Risk	Ad Hoc	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	4	1	2
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>6</b>	<b>1</b>	<b>4</b>

### CIO Self-Assessment

In Fiscal Year 2019, the National Capital Planning Commission (NCPC) made improvements in email security and multi-factor authentication. The NCPC focused efforts on email security to reduce the number of spam and phishing emails, which are known to be common attack vectors for federal networks and systems. In November 2018, NCPC enforced DMARC in response to BOD-19-01. The NCPC also applied email filters through Microsoft Office 365 threat protection policies. Additionally, NCPC worked with the DHS IPSS team to migrate to IPSSv2, which is configured to inspect inbound emails for known malware definitions.

To secure access to NCPC information and information systems, the NCPC enforced MFA for all NCPC network accounts and Microsoft O365 user accounts. Except for a few users who are awaiting PIV card issuance, staff are required to use their PIV cards and PIN to authenticate to the NCPC network. Similarly, Microsoft O365 users must use a one-time PIN code that is sent to their mobile devices.

There were two significant changes to the NCPC system inventory - one system was re-authorized, and one was decommissioned. The NCPC assessed and re-authorized the Microsoft Office 365 Multi-Tenant Cloud Information System in November 2018. The ATO is granted for three years and will expire in November 2021. In September 2019, the Authorizing Official determined the FMS did not meet the security requirements to continue operations. Therefore, the system was decommissioned on September 4, 2019.

Due to several factors, including limited technical resources, the federal government shutdown, and multiple reporting requirements that took priority, the NCPC was unable to make progress in security domains that were deemed at risk in FY 2019. In FY 2020, the NCPC will focus on managing risk in Configuration Management and Intrusion Detection and Prevention.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the National Capital Planning Commission (NCPC) was not performed for FY 2019, and the IG assessment section is marked "Not Applicable." 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 NCPC will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## National Council on Disability

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Optimized	Attrition	0	0	0
Protect	At Risk	Optimized	E-mail	0	0	0
Detect	At Risk	Optimized	External/Removable Media	0	0	0
Respond		Optimized	Impersonation	NA	0	0
Recover	Managing Risk	Optimized	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>1</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The National Council on Disability (NCD) in FY19 Q4 has taken additional action to meet the regulatory requirements to mitigate risk by implementing a customizable web application that acts as a central repository for NCD compliance findings, implementation details, vulnerability reports, and system inventory. This tool will replace the manual process of POA&M for NCD and will be used to track and collaborate on open findings. NCD will now be able to implement the FISMA framework with a built-in wizard to help make sure that no detail is overlooked. This will also help NCD keep track of artifacts and evidence that show compliance with various standards or show remediation of discovered findings or vulnerability scans. Lastly, it allows NCD to review statistics and generate reports in real time about security compliance.

### Independent Assessment

The National Council on Disability (NCD) information security program is deemed effective overall due to maintaining systemwide security policies and standards as the basis to assure information security. NCD's emphasis upon its protection of its information assets and enforcement of proper controls to ensure compliance with internal and external regulations uphold its system's security posture and reputation. NCD will continue development and maintenance of all agency programs designed to ensure the confidentiality, integrity and availability of its System Administration and agency information assets from unauthorized access, loss, alteration or damage while supporting the information sharing needs of the agency's environment.

# FY2019 Annual Cybersecurity Performance Summary

## National Credit Union Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	1
Protect	At Risk	Defined	E-mail	11	3	3
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Managed and Measurable	Improper Usage	5	7	3
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	9	21	4
			Web	3	7	0
			Other	6	4	5
			Multiple Attack Vectors	1	0	0
			<b>Total</b>	<b>35</b>	<b>42</b>	<b>16</b>

### CIO Self-Assessment

The National Credit Union Administration (NCUA) continues to improve the effectiveness of the information security program and will continue to strengthen the consistent implementation of policies, procedures, and strategies in 2020. While NCUA made progress in FY 2019, the following key risk areas are the most significant:

- 1) Data Management Security: NCUA established an Enterprise Data Governance Council that is charged with establishing data use standards, facilitating development of strategic objectives, and championing prudent data management practices. The initial focus of the Council is on a subset of the agency's data domains and will expand to other domains as the management of data matures.
- 2) Legacy Application Security: NCUA continues to progress with the enterprise business system modernization initiative, which includes replacing legacy systems, defining capabilities for a common platform to securely collect and share data, and building a data warehouse to enhance analytics and reporting using new business intelligence tools.
- 3) Insider Threat: NCUA's information and systems are vulnerable to compromise by an insider. Current capabilities may limit the timely detection of compromise or misuse of NCUA's information systems. NCUA is exploring additional protections through User and Entity behavior analytics (UEBA) which will accelerate detection and response capabilities to monitor known threats and behavioral changes in user data, providing critical visibility to uncover user-based threats.
- 4) HVAs: Three of NCUA's HVA's are legacy applications that will be modernized within the next five years. NCUA established a risk evaluation and threat assessment dashboard which provides a centralized, enterprise-wide view of information security risks across the organization with emphasis on HVAs. NCUA continues to conduct risk assessments of its HVAs and has improved capabilities in the area of threat detection, data protection, and incident response.

### Independent Assessment

The NCUA OIG assessed the NCUA in all Function areas and underlying Domains identified in the FY 2019 IG FISMA Reporting metrics as it pertain to the NCUA's six FISMA reportable systems and its overall information security program. The NCUA strengthened its information security program during FY 2019. Specifically, we determined the NCUA is effective in its security awareness and training program, contingency planning, and incident response program. In addition, the NCUA addressed and closed five of the eleven recommendations from the FY 2018 FISMA report. Furthermore, the NCUA is in the process of addressing and resolving the six remaining recommendations from the FISMA 2018 report.

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 risk management, access management, configuration management, and continuous monitoring, considering the compensating controls in place, we deemed NCUA's overall information security program effective. In addition, the weaknesses we identified during this year's evaluation do not have a significant enough impact on NCUA's overall information security program for us to consider it ineffective. The recommendations NCUA is making in the OIG's FY 2019 FISMA report should help the NCUA continue to improve the effectiveness of its information security program.

# FY2019 Annual Cybersecurity Performance Summary

## National Endowment for the Arts

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Defined	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	1	0
Recover	Managing Risk	Ad Hoc	Improper Usage	0	0	1
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	1
			Web	0	0	0
			Other	1	0	1
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>1</b>	<b>1</b>	<b>3</b>

### CIO Self-Assessment

A detailed assessment of the adequacy and effectiveness of the agency's information security policies, procedures, practices, and progress towards meeting the FY 2019 government-wide targets in the Cybersecurity CAP Goal metrics was performed. The National Endowment for the Arts (NEA) demonstrated improvement in enhancing its cybersecurity posture and closing over 80% of all prior year findings resulting from the OIG FISMA audits. The NEA conducted a series of phishing exercises, human trafficking, insider threat, and handling of PII/sensitive information training sessions using its automated security awareness program tools to expand the reach of our cybersecurity program. NEA measured the degree to which it was vulnerable to phishing. As a direct result of the targeted training, the NEA's phishing-prone score reflects a mere 3.8% likelihood of a successful attack, compared to an average score of 34.7% among other organizations of similar size and type. Despite this excellent result, we will stay focused in FY20 on continuous improvement of the NEA's cybersecurity risk posture.

### Independent Assessment

The information security program of the National Endowment for the Arts was evaluated as not effective. The NEA OIG contracted with an independent assessor to assess the effectiveness of the NEA's information security program and practices in FY 2019. The NEA has developed numerous policies and procedures to address prior year FISMA findings. As a result of the FY 2019 FISMA audit, the independent assessor has determined that areas of the NEA information security program still need improvement to become effective. Specifically, the assessor identified weaknesses in all IG FISMA metric domains. Thus, the assessor recommended the NEA to continue to improve its information security program. The IG maturity model considers Level 4, Managed and Measurable, as an effective level of overall security program. Based on the independent assessment of NEA's information security program, the overall maturity level results are between Level 1, Ad Hoc and Level 2, Defined.

# FY2019 Annual Cybersecurity Performance Summary

## National Endowment for the Humanities

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	1	0	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	0	0	0
			Loss or Theft of Equipment	1	3	1
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2</b>	<b>3</b>	<b>1</b>

### CIO Self-Assessment

For FY2019, the National Endowment for the Humanities (NEH) made significant improvements to its cybersecurity posture, which included security related to our two systems identified as HVAs and DHS BOD 18-01. Below is a list of the FY2018 risks and what work has been accomplished to address each:

FY18 risk: HVA systems that had automated flaw remediation solutions were only at 50% (1 of 2).

FY19 status: Now, 100% of the HVAs have automated flaw remediation solutions.

FY18 risk: The CAP Goal for Data Protection only met 3 of the 4 required metrics.

FY19 status: All HVAs feed into Central Enterprise Solutions, increasing the count to 4 of the 4 minimum required metrics.

FY18 risk: The CAP Goal of having 100% of second-level domains and mail-sending hosts have a DMARC policy setting of "reject." DHS BOD 18-01 was not met in FY18.

FY19 status: NEH now has 100% of second-level domains and mail-sending hosts configured with the DMARC policy setting of "reject" with 6 of the 4 metrics, successfully achieving the CAP goal for Intrusion Detection and Prevention.

FY18 risk: CDM is not fully in place.

FY19 status: NEH has been working closely with DHS and successfully piloted a small number of systems with CDM. NEH will continue to work DHS in rolling out CDM in FY20.

NEH has also been performing several system reviews, including a review of various system ATOs. The CIO continues to meet monthly with the agency's Senior Deputy Chairman, which has enabled us to secure funding to hire independent security assessors as part of the A&A of NEH's systems to include HVAs.

### Independent Assessment

The information security program of the National Endowment of 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 in previous fiscal years and competing priorities for NEH IT staff has contributed to the agency's inability to fully implement core elements of Risk Management (Identify), ISCM (Protect), and Contingency Planning (Recover), which impedes the overall effectiveness of the NEH information security program. Over the past year, the NEH has undertaken efforts to address recurrent FISMA findings and to remediate weaknesses concerning the agency's information security procedures and practices. Particularly, NEH leadership has approved the allocation of fiscal years 2019 and 2020 funding to support updated accreditation and authorization (A&A) of two core information systems. The A&A process for the first information system is in progress.

# FY2019 Annual Cybersecurity Performance Summary

## National Labor Relations Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	0	1
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	1	0	0
			Other	0	2	1
			Multiple Attack Vectors	1	0	0
			<b>Total</b>	<b>2</b>	<b>2</b>	<b>2</b>

### CIO Self-Assessment

The Agency contingency plan has been implemented. The National Labor Relations Board (NLRB) conducted contingency and incident response tabletop exercises facilitated by FEMA. The NLRB utilized an independent assessor (shared service) to test and validate the NLRB's SSP in accordance with NIST 800-53A revision 4. In addition, the Agency implemented CDM, Advanced Threat Protection and an automated tool for phishing exercises in FY19.

### Independent Assessment

The NLRB achieved a rating of "Consistently Implemented" for four out of the five security functions and "Managed and Measurable" for the remaining functions. Additionally, the NLRB also reduced the number of items at the "Ad Hoc" level from 18 items to 3 items, which represented a 83.3 percent decrease. This assessment marks a significant improvement over the prior year's assessment. However, because the NLRB is at the "Consistently Implemented" level for four of the five security functions, both the calculated and the assessed ratings are "Not Effective."

# FY2019 Annual Cybersecurity Performance Summary

## National Mediation Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

The National Mediation Board (NMB) made strides in better securing its information technology by taking numerous actions to meet Federal IT security requirements and industry best practices. NMB staff implemented Advanced Mobile Device Management to better manage its devices, implemented encryption to secure its public website, and implemented DHS Cyber Hygiene scanning of its publicly accessible websites to ensure the security of these systems. The NMB conducted its Cyber Awareness Challenge security training using a web-based training. To improve the security and maintainability of our office network, the agency updated its network firewalls and switches beginning at the end of FY 2018 and fully completed the project in early FY 2019. During the past fiscal year, the Agency has taken proactive steps toward lowering and mitigating cybersecurity risks. The agency has begun a complete rewrite and risk analysis of its cybersecurity policies, procedures, and documentation and is preparing to undertake a third-party risk analysis. The agency has contracted with a technical writer, an ISSO, and a security assessor. Working with the current staff, these IT professionals will review agency IT Security plans, procedures, and policy documents with the goal of bringing them into alignment and completeness.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the NMB was not performed for FY 2019, 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 IG Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. NMB has contracted with an independent assessor for FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## National Science Foundation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	2	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	5	2	2
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	1	0
			Loss or Theft of Equipment	0	0	0
			Web	15	3	0
			Other	11	1	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>33</b>	<b>7</b>	<b>3</b>

### 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 High Value Asset inventory based on its Mission Essential Functions related to grants management and merit review systems. NSF protects sensitive information and implements risk-based best practices to safeguard information from inappropriate access, use, or disclosure. NSF does not have a classified network. NSF continues to modernize and upgrade security tools to maintain enterprise-wide network visibility and situational awareness. NSF maintains 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

To assess whether the National Science Foundation (NSF) effectively implemented its agency-wide Information Security Program and practices, the independent auditors conducted a performance audit on behalf of NSF-OIG. The independent auditors performed detailed testing of NSF's Network General Support System (GSS) and United States Antarctic Program (USAP) GSS for compliance with selected NIST standards and other controls as specified in the FY 2019 Inspector General FISMA Reporting Metrics.

Based on our audit, NSF's Information Security Program was rated not effective for FY 2019. The driving factor for this assessment is the maturity of the USAP information security environment. Specifically, NSF did not ensure that: (1) USAP policies and procedures have been updated conform with current security requirements; (2) USAP vulnerability assessment policies and procedures clearly define milestones for patching of identified vulnerabilities; (3) USAP configuration management procedures require appropriate documentation of testing and approval for changes; and (4) USAP personnel perform appropriate monitoring for compliance with policies and procedures. Additionally, NSF did not ensure that existing identity and access management processes for user account disablement, account recertification, and on-boarding of new users, are being performed as designed by management.

To become more effective, NSF should ensure that USAP policies are updated to reflect current security requirements and ensure that monitoring and access management procedures are being performed as designed.

# FY2019 Annual Cybersecurity Performance Summary

## National Transportation Safety Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	1	3
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond	At Risk	Managed and Measurable	Impersonation	NA	0	0
Recover		Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	1	0	2
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>1</b>	<b>1</b>	<b>5</b>

### CIO Self-Assessment

The National Transportation Safety Board (NTSB) has completely replaced the EOL/EOS WAN equipment and built a new state of the art WAN infrastructure with direct connectivity to FedRAMP Authorized Cloud providers. Also, NTSB is in the process of replacing the EOL/EOS LAN equipment this quarter and the project is estimated to be completed by Q1 FY 2020. NTSB has completed the deployment of Zero Trust "VPN As a Service" platform and Cloud based Web content filter as a Service platform. Furthermore, NTSB has submitted a TIC 3.0 pilot use case to OMB/DHS for approval. NTSB has completed the deployment of CDM program Phase 1 and preparing for CDM Phase2 deployment.

### Independent Assessment

The scope of this audit covers the NTSB GSS. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of ISCM, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, 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 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

In accordance with last year's recommendations, DHS CDM program was implemented to provide SWAM, HWAM and Vulnerability data. Also, per last year's recommendations, BIA was drafted to complete the addition of RPO and RTO. Furthermore, NTSB plans to automate management of POA&Ms using a newly acquired GRC system per IG recommendations.

# FY2019 Annual Cybersecurity Performance Summary

## Nuclear Regulatory Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	3	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	2	0
Recover	Managing Risk	Managed and Measurable	Improper Usage	12	0	6
			Loss or Theft of Equipment	1	0	1
			Web	0	0	0
			Other	23	0	0
			Multiple Attack Vectors	1	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>40</b>	<b>2</b>	<b>7</b>

### CIO Self-Assessment

The agency needs to protect itself from cybersecurity risks generated by malicious actors and catastrophic events that impact the confidentiality, integrity, and availability of Nuclear Regulatory Commission (NRC) information systems and the agency's sensitive data. NRC has used risk assessments to develop and implement a proactive strategy to identify and mitigate risk to the agency. These actions include successfully implementing the controls, activities, and assets required by the DHS CDM program. The agency has a fully staffed and trained security operation center (SOC), a full-time incident response team, and a wide variety of skilled staff and contractors to implement, operate, and maintain other assets. From a programmatic stance, the NRC adheres to a governance program that leverages Federal Information Technology Acquisition Reform Act and ensures each system maintains an ongoing authority to operate. All cybersecurity role holders attend mandated specialized annual training and all Local Area Network account holders take annual computer security training. A daily situational awareness report that contains prior day events, current system status, and emerging issues is distributed, reviewed, and discussed at regularly held meetings with the CIO, CISO, and various levels of management and staff. The NRC SOC also uses a number of automated information services to ensure that the agency maintains up to date on threat intelligence data that helps the agency take a proactive approach to hunting unauthorized and potentially malicious behavior and issues across agency networks and to be aware of and take action before they become security events or incidents.

In summary, the NRC is aware of the risks facing the agency and takes the appropriate actions to ensure the information and information systems within remain secure. These steps and their results are reflected in the annual reports provided to OMB and DHS.

### Independent Assessment

NRC's information security program is effective. NRC has developed and established Enterprise Risk Management (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 authorization to operate (ATO) Continuous Monitoring Status Report, business impact assessment, 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 one, which is still under a periodic ATO. CDM Phase 2 has been completed and CDM Phase 3 is in the process of being implemented.

# FY2019 Annual Cybersecurity Performance Summary

## Nuclear Waste Technical Review Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Managed and Measurable	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

As of FY19, the most prevalent cybersecurity risk to the Nuclear Waste Technical Review Board (NWTRB) has been attempts to access cloud-based email services by foreign actors. The NWTRB took additional steps to secure this resource using vendor provided smart lockout features and geolocation-based access policies, creating a more robust layered defense of email services. The agency has continued to maintain sound cyber-hygiene practices, ensuring that all systems and workstations are patched regularly. In FY19, the agency possessed zero critical/high vulnerabilities older than 14 days on all systems and workstations. Additionally, the NWTRB had no cyber incidents in the fiscal year. A security awareness training was performed for all users to improve awareness and understanding of the importance of security practices. Additional cybersecurity concepts are included in regularly held meetings to further reinforce the need for good security. The agency continues to prioritize the need for sound cybersecurity practices through assessments to identify areas of strengths and improvements, and acting upon those findings.

### Independent Assessment

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 to best decide on how resources are spent in the protection of assets. The agency has achieved a Fully Defined maturity level across all function areas as a baseline and is moving towards the Consistently Implemented maturity level for all function areas. Based upon an independent third-party assessment, the agency security program was found to be effective overall. The agency was able to meet the Consistently Implemented maturity level or higher across all function areas. Of the fifteen findings identified by the assessment, there were no High Risk findings, with nine Low Risk and six Moderate Risk. These findings and associated recommendations were developed into POA&Ms for remediation in FY20. Moving forward, NWTRB will seek to further improve through the maturity model levels as appropriate in consideration of agency constraints and risk.

# FY2019 Annual Cybersecurity Performance Summary

## Occupational Safety and Health Review Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Optimized	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The Occupational Safety and Health Commission (OSHRC) assessment of the cybersecurity risks originate from existing collaborative relationships with Einstein, CDM Dashboard, MISA, US-CERT scans, as well as internal endpoint clients and system firewall appliances. During FY 2019, OSHRC mitigation efforts have purely been in a reactive/proactive approach as risks are identified. Based on notifications from the many monitors in place, OSHRC evaluates the relevance of the risks against existing systems, reacts accordingly to the risk, and decides whether a preemptive action is necessary. OSHRC has not had a violation as a result of a cybersecurity risk in FY 2019.

### Independent Assessment

The information security program of the Occupational Safety and Health Review Commission was evaluated as effective.

**Identify:** The overall rating is due to the need to finalize policies and related documents. Procedures are currently in place and in varying states of implementation.

**Protect:** The overall rating is due to PIV card implementation in process. Policies are in draft and are being finalized, procedures in place are in varying states of implementation, and the tailoring of training in a small organization is not cost effective.

**Detect:** The overall rating is due to policies being finalized, while procedures are in place and in varying states of implementation.

**Respond:** No additional information.

**Recover:** The Overall rating is primarily due to implementing supply chain risks and metrics on effectiveness.

# FY2019 Annual Cybersecurity Performance Summary

## Office of Government Ethics

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Managed and Measurable	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

In FY 2019, the U.S. Office of Government Ethics (OGE) engaged an independent assessor to assess the status of OGE's internal network in accordance with NIST SP 800-37 Revision 1, NIST SP 800-53, Revision 4, and NIST SP 800-53A, Revision 4. No "critical" or "high" risk findings were identified. 35 findings were identified by the assessor as "moderate risk." 13 findings were identified as "low risk." The OGE Chief Information Officer (CIO) has written a Plan of Action and Milestones (POAM) document for each deficiency. Each deficiency has been documented, assigned an ID, and is being tracked until mitigated or accepted by the Authorizing Official (AO). Each POAM will be signed by the CIO and the AO to indicate either closure or risk acceptance. In addition, OGE also procured an independent evaluation of its information security program using FY 2019 IG FISMA reporting metrics. The purpose of this audit was to determine the effectiveness of the agency's information security program and practices. This fiscal year's audit represents the first time OGE's information security program has been evaluated against these requirements. For purposes of the IG FISMA Metrics Audit, DHS defined five levels of maturity. The high-level result of OGE's FY 2019 IG FISMA Metrics Audit is "Managing Risk" in all levels of maturity, yielding an overall rating of "Managing Risk."

### Independent Assessment

The independent auditor found the Office of Government Ethics' (OGE) information security program to be effective. As a micro-agency, OGE has a small IT footprint. OGE's systems are actively managed by a small and skilled Federal staff dedicated to maintaining the confidentiality, integrity and availability of their systems. OGE has opportunities for improvement in each of the Domains, specifically with regards to automation; however, manual efforts presently address the intent of those controls. Deployment of automated toolsets in select focus areas is presently not feasible due to budgetary constraints. OGE forecasts increased adoption of cloud services, in addition to enhancements to existing processes to solidify Domain maturity levels.

# FY2019 Annual Cybersecurity Performance Summary

## Office of Navajo and Hopi Indian Relocation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	Managing Risk	Ad Hoc	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	1	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>1</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

An assessment shows the Office of Navajo and Hopi Indian Relocation (ONHIR) had the following cybersecurity risks:

- HVA had unencrypted data at rest;
- Lack of multi-factor authentication;
- Lack of security report posing security risks in instances such as logon and logoff of privileged accounts, object-level authority, system values, values of users on the system;
- The network security lacked PIV usage and has endpoints with Windows 7;
- The Agency website software was out of date;
- Minimal content filtering

In FY19, the Agency has researched and procured a Managed Security Service for the HVA, encrypted all PII data fields in the HVA and installed multi-factor authentication. For the Agency network, ONHIR replaced many of the Windows 7 workstations with Windows 10. User PIV cards are required and content filtering has been tightened. The Agency website has been revamped with an up-to-date 508 compliant hosting.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the ONHIR was not performed for FY 2019, and the IG assessment section was marked "Not Applicable." 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 ONHIR will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Office of Personnel Management

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	18	0	4
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Defined	Improper Usage	38	123	156
			Loss or Theft of Equipment	24	8	10
			Web	3	1	0
			Other	109	28	57
			Multiple Attack Vectors	8	0	1
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>200</b>	<b>160</b>	<b>228</b>

### CIO Self-Assessment

OCIO made significant progress in overcoming the staffing and resource challenges that have restrained the program in recent years. These challenges were addressed with respect to risk assessments for major information systems, complete and comprehensive testing of security controls, and consistent implementation of OPM's Information Security Continuous Monitoring activities. Senior leadership vacancies were filled early in the year and staffing shortfalls were documented in order to identify additional resource constraints. Senior agency leadership has taken steps to ensure that critical positions within OCIO are funded and allocated. The CISO office maintained current Authorizations to Operate (ATOs) throughout FY 2019 for all OPM but one information system.

The Agency made significant improvements in Security Training in FY 2019. The agency-wide IT security awareness training program required by all Government employees and contractors contributed to this improved score as well as the enhanced tailored training for employees with significant security responsibilities. Improvements to the latter will continue in FY 2020.

With the release of OMB M-19-17 which supersedes M-11-11 and includes new ICAM requirements, OPM will identify steps to implement the requirements of M-19-17.

### Independent Assessment

The information security program of the U.S. Office of Personnel Management was evaluated as not effective. In FY 2019, 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 FY 2019.

# FY2019 Annual Cybersecurity Performance Summary

## Office of Special Counsel

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	0	2
			Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	1	0
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>1</b>	<b>2</b>

### CIO Self-Assessment

The Office of Special Counsel (OSC) has actively been reviewing its cybersecurity risk management program. In FY19, OSC had a complete turnover in IT staff to include the CIO, CISO, helpdesk, and cybersecurity personnel. The new IT staff is working to update and modernize the Cybersecurity Program to include implementing consistent and thorough policies to improve the OSC's cybersecurity posture. This FY, OSC IT staff enabled features in the cloud environment to provide for additional layers of protection to email traffic, as well as a refresh to the intrusion detection and prevention solutions to the enterprise. OSC worked diligently with DHS to implement CDM Phase One. OSC is committed to further strengthen and enhance the Cybersecurity Program in the upcoming fiscal year.

### Independent Assessment

OSC continues to work towards hardening the security posture of the GSS environment. OSC has complied with most security control requirements tested during the security assessment of the OSC information security program and OSC information systems. Furthermore, 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 mechanisms that provide on demand and real-time baseline, security configuration requirements, and risks views of the entire agency infrastructure;
- Automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, ISCM, and Configuration Management 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 Incident Response program that includes validated processes for responding, containing, and reporting security incidents to oversight agencies such as US-CERT and DHS;
- OSC has established and defined a Contingency Planning program that includes a Business Impact Analysis (BIA), Contingency Plan, and Continuity of Operations Plan for its main General Support System (GSS) network.

Findings and Recommendations from the most recent audit report have been converted to POAMS and are actively being corrected and implemented by the OSC Cybersecurity Team thus resulting in significant improvements.

# FY2019 Annual Cybersecurity Performance Summary

## Office of the Comptroller of the Currency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	2	13	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	1	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	8	0	10
			Loss or Theft of Equipment	1	8	0
			Web	1	0	0
			Other	4	7	3
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>16</b>	<b>29</b>	<b>13</b>

### CIO Self-Assessment

Key risks for the Office of the Comptroller of the Currency (OCC) continue to include: security breaches and cyber exploits caused by personnel error; network exploits caused by unauthorized devices and advanced persistent threats (APTs); and disruption of mission essential functions caused by system failure.

Security breaches and cyber exploits caused by personnel error: The OCC continued its end user education campaign on five cybersecurity risks, with a priority on weekly phishing exercises, follow-up instruction for 'phished' users, and individual accountability measures. It improved end user security both on and off-network by adding endpoint controls for signature-based threat detection & prevention and malware quarantining; preventing uploads and copy/paste off-network; and cloud-based vulnerability scanning and reporting.

Unauthorized devices and advanced persistent threats (APTs): The OCC continued implementation of CDM network access control technology to enhance its ability to eliminate rogue devices and enforce device configuration compliance. OCC implemented enterprise logging enhancements to improve its event correlation and analysis as well as its incident response capabilities. The OCC also engaged the services of an intelligence-led security company to conduct an independent assessment of its network environment, which identified no APT indicators.

Mission essential function disruption: OCC business continuity and resiliency management activities to mitigate mission disruption included a full functional disaster recovery test, two isolation tests, and enhanced outreach and training in information system contingency planning to links these plans to agency continuity of operations activities. These actions contributed to the overall "Managing Risk" rating assessed by OMB and DHS for the OCC's CIO FISMA metrics, and a Level 4 maturity rating in the Treasury OIG's annual FISMA audit.

### Independent Assessment

The information security program of the Office of the Comptroller of the Currency was evaluated as effective. Key risks for the OCC continue to include: security breaches and cyber exploits caused by personnel error; network exploits caused by unauthorized devices and APTs; and disruption of mission essential functions caused by system failure.

Security breaches and cyber exploits caused by personnel error: The OCC continued its end user education campaign on five cybersecurity risks, with a priority on weekly phishing exercises, follow-up instruction for 'phished' users, and individual accountability measures. OCC improved end user security both on and off-network by adding endpoint controls for: signature-based threat detection & prevention and malware quarantining; preventing uploads and copy/paste off-network; and cloud-based vulnerability scanning and reporting.

Unauthorized devices and APTs: The OCC continued implementation of CDM network access control technology to enhance its ability to eliminate rogue devices and enforce device configuration compliance. It implemented enterprise logging enhancements to improve its event correlation and analysis as well as its incident response capabilities. The OCC also engaged the services of an intelligence-led security company to conduct an independent assessment of its network environment, which identified no APT indicators.

Mission essential function disruption: OCC business continuity and resiliency management activities to mitigate mission disruption included a full functional disaster recovery test, two isolation tests, and enhanced outreach and training in information system contingency planning to links these plans to agency continuity of operations activities. These actions contributed to the overall "Managing Risk" rating assessed by OMB and DHS for the OCC's CIO FISMA metrics, and a Level 4 maturity rating in the Treasury OIG's annual FISMA audit.

# FY2019 Annual Cybersecurity Performance Summary

## Overseas Private Investment Corporation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	2	2	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Defined	Improper Usage	0	0	1
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	8	9	10
			Web	1	0	0
			Other	3	2	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>14</b>	<b>13</b>	<b>11</b>

### CIO Self-Assessment

While the Overseas Private Investment Corporation (OPIC) does not have HVAs, it has determined its greatest cybersecurity risks are untimely remediation of hardware and software vulnerabilities, incomplete implementation of MFA for privileged accounts and for access to O365, and lack of detection of unauthorized assets. To mitigate the risk of untimely remediation of hardware and software vulnerabilities, OPIC has developed and implemented five main customized processes for patching varying types of vulnerabilities based on their severity levels, degree of deviation, and/or status during out-of-cycle patch scheduling. In parallel, the Agency has invested and installed an enterprise-wide vulnerability management solution to automate most of its patches identified through robust routine scans of its network assets. To address the incomplete implementation of MFA, OPIC has developed a plan to enforce MFA on all privileged user accounts and for all O365 access vectors as part of the Agency's infrastructure upgrade. Meanwhile, OPIC continues to implement MFA to both on-site and remote network access, perform detailed and periodic account reviews, and train users to identify malicious emails designed to obtain network credentials. The Agency is also in the process of modifying its password policy, which would require network account users to select even stronger passwords in alignment with NIST guidance. To mitigate the risk of unauthorized assets, OPIC locks down network access points and collaborates with third-party vendors to determine automated methods for detecting the use of rogue hardware and software on the Agency's network.

### Independent Assessment

OPIC's information security program was evaluated as part of the FY 2019 FISMA Audit. This audit included an evaluation of three out of three FISMA reportable systems at OPIC. The FY 2019 FISMA Audit noted 56 of 70 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 a few recommendations made to help OPIC improve their information security program. These recommendations can be found in the FY 2019 FISMA Audit report.

# FY2019 Annual Cybersecurity Performance Summary

## Peace Corps

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	10	19	13
			Loss or Theft of Equipment	1	1	0
			Web	0	0	0
			Other	1	5	8
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>12</b>	<b>25</b>	<b>21</b>

### CIO Self-Assessment

In FY19, Peace Corps (PC) took the following actions to reduce risk across the following cybersecurity domains:

1. Security Domain: Asset Management - The Agency implemented centralized software management tools, completed Phase 1 of the CDM Program, and has started to populate the agency and federal dashboard. Additionally, the agency has implemented a global capability to restrict the connection of unauthorized hardware assets to its network.
2. Remote Access Protection - The Agency completed deployment of its centrally managed, FIPS 140-2 compliant encrypted VPN tunnels to all 58 of its international posts.
3. Credentialing and Authorization - The Agency is awaiting DHS PMO support on deployment of CDM Phase 2. However, it has installed dynamic role-based authentication services and approved funding for MFA infrastructure for its global posts.
4. Exfiltration and Enhanced Defenses - The Agency has procured tools to support its implementation of data loss prevention and is on target to begin initial deployment of the solution in FY20.
5. Respond and Recover - The Agency addressed BOD 19-01 Mitigate DNS Infrastructure Tampering and BOD 19-02 Vulnerability Remediation requirements. The agency migrated from an on-premises data center to a managed, state-of-the-art data center, which provided dramatically improved security controls and redundancy. It should be noted that FY19 also saw the implementation of a cloud-based disaster recovery environment. This environment is scheduled to be operational in Q1 of FY20.

### Independent Assessment

Our assessment reflects that the PC lacks an effective information security program, as DHS and OMB consider Level 4, Managed and Measurable, to be an effective level of security for the overall program. Based on the assessment of the PC's information security program, the overall maturity level results are in between Level 1, Ad-hoc, and Level 2, Defined. As such, we identified issues relating to the people, processes, technology, and culture aspects across all the CSF Function areas. Moving forward, involvement from all levels of the Peace Corps leadership is needed to advance and fully develop its information security program.

# FY2019 Annual Cybersecurity Performance Summary

## Pension Benefit Guaranty Corporation

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Consistently Implemented	E-mail	2	0	0
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	1	1	3
			Loss or Theft of Equipment	0	0	0
			Web	1	0	0
			Other	2	0	1
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>6</b>	<b>1</b>	<b>4</b>

### CIO Self-Assessment

The Pension Benefit Guaranty Corporation (PBGC) is responsible for protecting pension benefits and data privacy of plan participants. Protecting PBGC's networks, systems, and data has been a long-standing and continuous management challenge. Thus, data protection continues to be a priority given the high volume of PII in PBGC's possession. In addition, security domains within the CSF functions falling short of the "effective" threshold per fiscal year OIG FISMA audit engagements, remain challenges and potential risks. Further improvements in PBGC's information security posture are needed so that the Corporation can remain agile in the rapidly changing threat environment. Management has recognized these challenges and will continue to work collaboratively with the PBGC OIG.

In the past fiscal year, cybersecurity risks have been mitigated and security and privacy controls have been strengthened due to enhanced compliance and oversight. PBGC managed identified risks by developing and implementing risk mitigation plans, creating POA&M, and accepting risks where operational constraints exist. Additionally, programmatic strategies and approaches were employed and ensured PBGC systems were compliant with the Corporation's Information Security Program and applicable laws and regulations. PBGC continued to mature its enterprise risk management practices and improved risk-based prioritization of its resources by briefing executives from each business unit about cybersecurity risks impacting their programs. The CIO continued to sponsor 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. Significant progress has been made over the past year in managing information risk.

### Independent Assessment

The PBGC OIG contracted with an independent auditor to determine degree of compliance for PBGC's information security programs and practices with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance. This audit assessed the maturity of PBGC's information security program using the FY 2019 IG FISMA metrics under OIG oversight.

In FY 2019, the independent auditor reviewed a sampled five systems. The independent auditor noted improvements to PBGC's ISCM program that raised the maturity of the detect function to the effective level of managed and measurable. PBGC's maturity of the respond function remained at the effective level of managed and measurable. The three other functions, however, were evaluated at the consistently implemented level; therefore, PBGC's overall information technology security program was rated as not effective. Our detailed report and recommendations will be available in our audit report of PBGC's FY 2019 compliance with FISMA.

# FY2019 Annual Cybersecurity Performance Summary

## Postal Regulatory Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
			Loss or Theft of Equipment	0	0	0
<b>Overall</b>	<b>At Risk</b>		Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

During this past year, the Post Regulatory Commission (PRC) has taken several steps to improve the overall security and performance of PRC systems and IT Infrastructure. With new security threats continually emerging, the Commission continues to enhance 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. In addition, the Commission conducted a penetration and phishing exercise utilizing DHS CISA's assessment services. The results of the assessment provided the Commission with detailed security findings identifying high-risk areas of concern. This allowed the Commission IT staff to quickly address the findings without impact to budget or other resources and improve the security posture of PRC IT infrastructure. In partnering with DHS security assessment services, CDM, and other security programs such as Einstein 3(a) and Managed Trusted Internet Protocol Service (MTIPS), the Commission greatly improved its 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 PRC was not performed for FY 2019, and the IG assessment section is marked "Not Applicable." 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 PRC's IG will explore contracting with an independent assessor in FY 2020 .

# FY2019 Annual Cybersecurity Performance Summary

## Presidio Trust

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	High Risk	Ad Hoc	E-mail	0	0	3
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	0	0	1
			Web	0	0	0
			Other	0	0	1
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>5</b>

### CIO Self-Assessment

The Presidio Trust is a small, wholly-owned government corporation that has unique mandates under the Presidio Trust Act for property and fiscal management.

The Trust's security programs goals focus on reducing cybersecurity risks which could affect the confidentiality of PII for tenants and staff, integrity of property management and financial data, and availability of technology systems supporting the Trust's mission while aligning with federal guidance for agency security programs. The Trust continues to evaluate and reduce risk, whether it originates externally or internally, from natural disasters, accidental or intentional events.

In FY19, the Trust has made considerable progress in several foundational areas to reduce risk:

- Developed a comprehensive security policy with associated procedures.
- All employees are trained in cybersecurity topics.
- Desktop computers have been upgraded to the most modern and secure Windows operating system.
- Strengthened authentication practices into several federal systems.
- Developed an ability to recover key systems into the cloud in the event of a disaster.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Presidio Trust was not performed for FY 2019, and the IG assessment section is marked "Not Applicable." Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the IG 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 in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## Privacy and Civil Liberties Oversight Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Managed and Measurable	E-mail	0	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### 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. The Board has made significant progress towards implementing NIST controls to mitigate risks to IT assets, environment, and mission-critical functions from cyber-attacks. The FY 2019 independent audit validated the Board's efforts through a determination of no findings of selected controls. Also, the Board achieved full compliance with DHS BOD 19-01 and 19-02 and suffered no major information security incidents in FY 2019.

The Board aggressively worked to remediate FY 2018 FISMA audit findings. The Board closed seventy-five percent of FY 2018 independent audit findings. The FY 2018 independent assessment also identified the need to conduct a disaster recovery test. The Board successfully conducted a disaster recovery test in FY 2019.

Additionally, the Board enhanced its security posture and situation awareness by implementing capabilities to detect vulnerabilities and mitigate attacks. The Board conducted an independent security penetration test and phishing exercise to identify and resolve gaps. The Board will continue to leverage shared service providers along with DHS CDM and Managed Trusted Internet Protocol Service providers to identify and contain threats as well as prioritize risks.

### Independent Assessment

The information security program of the PCLOB 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 is proactive in remediating all identified deficiencies and strengthening existing security controls. The results of the FY 2019 independent audit identified no findings for selected controls. The PCLOB successfully closed seventy-five percent of FY 2018 findings.

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 exhibit "a better than average external and internal vulnerability profile," indicating effective implementation FISMA security controls. The PCLOB has fully implemented MTIPS across the enterprise and continues to steadily increase their security posture across all cybersecurity CAP goal targets.

# FY2019 Annual Cybersecurity Performance Summary

## Railroad Retirement Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	5	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	20	23	21
			Loss or Theft of Equipment	25	24	18
			Web	2	0	0
			Other	13	4	20
			Multiple Attack Vectors	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>65</b>	<b>51</b>	<b>59</b>

### CIO Self-Assessment

The CIO and CISO recognize the Railroad Retirement Board (RRB) cybersecurity program is still in need of improvement and acknowledges the cybersecurity risks identified in the five domains in the recent FY 2019 FISMA audit conducted by the RRB's OIG. Our goal is to remediate those cybersecurity risks as soon as possible. Specifically, the CIO and CISO plan to address the findings in the five NIST CSF domains in the recent audit:

The CIO and CISO concur that a fully integrated enterprise-wide Risk Management Program is required for the RRB to manage risk effectively. The CISO plans on developing a RMF and communicating the responsibilities to all information system owners at the next quarterly ISPC. The following RMF responsibilities will be discussed at the ISPC meeting:

- Develop and maintain an up-to-date inventory for all the information systems
- Develop the responsibilities of the information system owners risk management activities and develop an RMF checklist for the information system owners to follow

The CISO understands the importance of updating and reviewing the RRB's Information Security policies and procedures and over the past year these policies have been updated. The Risk Management policy and procedures are included in the review. The updated Risk Management policy and procedures will include the roles and responsibilities for all of the information system owners.

### Independent Assessment

To assess how the RRB established and implemented its agency-wide Information Security Program and practices, as required by FISMA, an independent auditor performed detailed testing of RRB's Agency Enterprise General Information System, Benefit Payment Operations, Financial Management Integrated System, Financial Interchange, and HR Links systems and applications for compliance with selected controls from NIST SP 800-53, Revision 4. Overall, the Information Security Program was ineffective and rated "Level 1 - Ad Hoc" for the NIST CSF in Identify, Detect, and Recover and achieved a "Level 2 - Defined" for the CSF domains of Protect and Respond. Continued management attention is necessary in all functions, as the independent auditor identified that RRB scored below the "consistently implemented" level in multiple security metrics within all functions.

# FY2019 Annual Cybersecurity Performance Summary

## Securities and Exchange Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	1	0	1
Protect	Managing Risk	Defined	E-mail	336	339	249
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Managed and Measurable	Improper Usage	48	100	57
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	2	1	0
			Web	65	36	24
			Other	63	74	61
			Multiple Attack Vectors	12	2	4
			<b>Total</b>	<b>527</b>	<b>552</b>	<b>396</b>

### CIO Self-Assessment

The Securities and Exchange Commission (SEC) completed several initiatives in FY 2019 to further improve its cybersecurity posture. This included increased emphasis on HVA risk management, upgraded threat protection technologies, remediation of auditor recommendations, and enhanced awareness training. In accordance with OMB memo 19-03, the SEC designated an integrated agency-level governance structure, led by the COO, to enable the incorporation of HVA activities into broader agency planning activities for information system security and privacy management. In accordance with BOD 18-02, DHS conducted security testing for high value assets. Penetration tests and security assessments were conducted by third party cybersecurity experts for numerous SEC systems. Improvements were made to security operations capabilities during FY 2019, which included upgrades to perimeter and host-based threat detection and mitigation devices. Additionally, the SEC enhanced its ability to detect vulnerabilities within source code. The SEC further implemented the NIST Cybersecurity CSF in accordance with an Executive Order by completing risk profiles for all HVAs. In FY20, the SEC will continue to integrate the CSF into its cyber risk management practices. The SEC completed corrective actions sufficient to close twenty-four audit recommendations issued by the OIG and seven audit recommendations issued by the GAO. The SEC enhanced its information security and privacy training and awareness program by achieving 100% compliance with annual privacy and security training for staff and conducting staff-wide phishing exercises. Continued progress was made toward implementing DHS CDM capabilities by establishing agency-level dashboard components that will be used to collect data from security management tools and interface with the Federal-level CDM dashboard.

### Independent Assessment

The U.S. SEC made progress in implementing information security policies and procedures to address security risks at the organizational level. Specifically, the Commission created an entity-wide Identity and Access Management strategy, enhanced its security awareness and training processes, continued its efforts to enhance its continuous monitoring program, and improved its incident response capabilities. Although SEC made program improvements, the agency continued to face challenges with improving software asset management, assuring Information System Owners performed assigned responsibilities, enforcing strong authentication mechanisms, enhancing its configuration management activities, improving the timeliness of security patch deployments, and delivering specialized security training. As a result, the independent assessors determined that the SEC's information security program did not meet the definition of "effective."

# FY2019 Annual Cybersecurity Performance Summary

## Selective Service System

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	1	0	0
Detect	Managing Risk	Consistently Implemented	External/Removable Media	0	0	0
Respond		Managed and Measurable	Impersonation	NA	0	0
Recover	At Risk	Defined	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	59	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>60</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The DHS BOD 18-02 HVA assessments concluded that additional controls are required to make protection more robust and sustain the current HVA infrastructure. The 2019 annual FISMA IG report identified additional NIST compliance issues that Selective Service System (SSS) is actively remediating along with DHS 18-02 POA&Ms. Systemic risks for infrastructure equipment and personnel resources were identified in the FY20 budget proposal and additional funding will mitigate Cybersecurity compliance issues.

### Independent Assessment

The information security program of the Selective Service System was evaluated as not effective. SSS did not take corrective action to address most of the IT security program deficiencies that impacted the agency's IT security program in FY 2018. Internal control breakdowns in the agency's IT security program pose a serious vulnerability to SSS's information and information systems. We attributed these conditions, in part, to: (1) the need for a more effective corrective action program as outlined in OMB Circulars A-123, A-50, and other OMB directives; and (2) significant changes in OCIO management within the agency over the last several years. As a result, control functions related to the CSF had flaws, were not effectively implemented, and oversight and monitoring of the agency's IT security program was insufficient, thereby increasing the risk to the agency's information and information systems that store sensitive PII information.

The Deputy Director provided a written response to the audit report, dated October 2, 2019, which states that SSS accepted the report's findings and has developed "...detailed remediation action plans that will be tracked through POA&Ms until completion in early 2020." The Deputy attached an audit response memorandum that summarizes the actions to be taken and targeted completion dates. While we have not audited the details provided in this response, the actions contemplated, if carried through to completion, should address the related report's findings and recommendations.

# FY2019 Annual Cybersecurity Performance Summary

## Small Business Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	1	1	4
Protect	At Risk	Defined	E-mail	1	135	1,100
Detect	Managing Risk	Defined	External/Removable Media	0	0	6
Respond		Managed and Measurable	Impersonation	NA	0	7
Recover	Managing Risk	Consistently Implemented	Improper Usage	6	45	134
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	39	16	6
			Web	14	19	139
			Other	80	128	368
			Multiple Attack Vectors	3	0	1
			<b>Total</b>	<b>144</b>	<b>344</b>	<b>1,765</b>

### CIO Self-Assessment

Throughout the year, the SBA continued to build a robust, adaptable, and cost-effective Cybersecurity Program. Notable efforts included deploying Enterprise Cybersecurity Services across the agency, demonstrating innovative techniques to shape the TIC 3.0 initiative, implementing major CDM components in the cloud, and enhancing endpoint security capabilities through our Windows 10 deployment. In addition to the above intrinsic Cybersecurity benefits, these projects are reflected through our steady CAP Goal improvement and RMA rating.

### 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, OIG evaluated the design, implementation, and operating effectiveness of SBA's information security policies, procedures, and practices. OIG determined that SBA has established and maintained its information security program and practices for the eight FISMA metric domains. In addition, SBA improved its incident response program to be rated as "Managed and Measurable" and is operating in an effective manner. However, the other seven domains of the program reflected deficiencies that we identified were not fully effective. We made new recommendations in these seven domains, and while SBA has worked to implement recommendations from previous FISMA reports, challenges remain in implementing an effective IT security program.

# FY2019 Annual Cybersecurity Performance Summary

## Social Security Administration

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	81	66	267
Protect	Managing Risk	Defined	E-mail	112	67	90
Detect	Managing Risk	Defined	External/Removable Media	5	0	5
Respond		Defined	Impersonation	NA	2	13
Recover	Managing Risk	Defined	Improper Usage	1,059	1,547	1,462
			Loss or Theft of Equipment	79	38	35
			Web	349	501	560
			Other	1,236	1,147	2,353
			Multiple Attack Vectors	23	1	11
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>2,944</b>	<b>3,369</b>	<b>4,796</b>

### CIO Self-Assessment

SSA's 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. In FY 2019, SSA made substantial improvements and progress in securing applications, leveraging the cloud, managing assets and vulnerabilities, strengthening network and incident response capabilities, improving security training, and enhancing the overall effectiveness of the cybersecurity program.

Specifically, in the Identify area of the NIST framework: SSA established a methodology for scoring risks (to include measuring risk appetite and tolerance) via a new Risk Management Framework strategy. In the Protect area: SSA concentrated on mitigation efforts surrounding unauthorized software to include policy enforcement; removing instances of unauthorized software from our network; and reporting any instances of unauthorized software to senior agency leadership. SSA also accelerated planning efforts to fast track technical enforcement for software whitelisting. In the Detect area: SSA continued implementing an Agency Security Information and Event Management (SEIM) tool, expanding functionality and onboarding more systems to monitor the enterprise. In the Respond area: SSA updated and published an official Agency incident response plan. In the Recover area: SSA updated regional office and component Continuity of Operations plan templates with references to reflect current guidance and conducted annual business continuity testing in accordance with federal requirements.

### Independent Assessment

The information security program of SSA was evaluated as not effective. Although SSA established an Agency-wide information security program and practices, an independent public accounting (IPA) firm identified 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 its information and information systems. In addition, the IPA did not assess any of the FISMA domains as Managed and Measurable. The FY 2019 FISMA IG Reporting Metrics defines an effective information security programs as Managed and Measurable.

# FY2019 Annual Cybersecurity Performance Summary

## Surface Transportation Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Defined	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	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
<b>Overall</b>	<b>Managing Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The Surface Transportation Board (STB) has been working hard to improve its information security program and remains committed to exceeding the bar set by the CIO FISMA Metrics. The Board continues to make steady improvements to mitigate and manage information security risk. The STB has developed risk-related policies and procedures and has addressed risk through its Risk Management Committee, which meets at least quarterly. The Board has taken steps to protect its information systems by implementing technical controls that block unauthorized endpoints from connecting to the Board's networks, enforcing PIV authentication for access to STB systems and office spaces, and securing connections to external networks for STB personnel. The Board has also implemented a process of vulnerability detection and mitigation that decreases the information system attack surface of the STB. The Board has standardized its incident response procedures to comply with DHS US-CERT incident response best practices and guidance.

### Independent Assessment

For the FY 2019 audit, STB's information security program and practices were evaluated based on a representative sample of its information systems. Specifically, the General Support System and two cloud-based systems. The FY 2019 audit covered the period from October 1, 2018 to May 31, 2019.

Based on the audit procedures performed, it was concluded that STB's information security program remains ineffective as the agency continues to make progress in maturing its overall information security program through the development of its policies and procedures to address prior year recommendations. While STB has made significant efforts to address previously identified issues, additional work is needed to define and implement an effective information security program.

In summary, 13 recommendations were closed and 8 remain open at the conclusion of the FY 2019 audit. New recommendations were not developed for the 5 functions as the issues identified within these functions for FY 2019 audit were consistent with those identified in the prior year.

At the conclusion of the FY 2019 audit, STB's information security program was rated at a Level 2, Defined.

# FY2019 Annual Cybersecurity Performance Summary

## Tennessee Valley Authority

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Managed and Measurable	E-mail	0	1	0
Detect	Managing Risk	Defined	External/Removable Media	1	0	0
Respond		Managed and Measurable	Impersonation	NA	1	1
Recover	Managing Risk	Consistently Implemented	Improper Usage	13	7	2
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	9	17	4
			Web	7	0	0
			Other	5	2	15
			Multiple Attack Vectors	0	0	1
			<b>Total</b>	<b>35</b>	<b>28</b>	<b>23</b>

### CIO Self-Assessment

The Tennessee Valley Authority (TVA) works continually to identify and mitigate its cybersecurity risks. In FY 2019, its assets and functions were susceptible to unauthorized network connections and vulnerable software, posing the highest risk to TVA. To mitigate these throughout FY 2019, TVA nearly 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 coming years. To mitigate the risk of insecure software, TVA Cybersecurity implemented ongoing active and passive scanning capabilities on its corporate network during FY 2018. During FY 2019, TVA enhanced 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 Cloud Access Security Broker solution to monitor TVA's information in the cloud. Technical testing and implementation continued in FY 2019 and will conclude in the coming years. Finally, TVA has implemented user behavior analytics and has established an insider threat working group comprised of TVA Cybersecurity, Police, Human Resources, General Counsel, and the 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. TVA operates an effective information security program and will continue to use a risk-based approach to prioritize security maturity and make appropriate investments in order to protect its mission and operations.

### Independent Assessment

Based on the analysis of the metrics and associated maturity levels defined by FISMA, and using IG discretion, the auditors found TVA's information security program was not operating in an effective manner. In addition, analysis of the metrics revealed three of the five functions were below the prescribed level (Managed and Measurable) to be considered effective. 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 to ensure compliance with FISMA and applicable standards, including guidelines issued by OMB and NIST. Our scope was limited to determining the maturity level of each metric as defined in the FY2019 IG FISMA Reporting Metrics.

# FY2019 Annual Cybersecurity Performance Summary

## U.S. Trade and Development Agency

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	Managing Risk	Defined	E-mail	0	1	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	1	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>2</b>	<b>0</b>

### CIO Self-Assessment

In the last fiscal year, U.S. Trade and Development Agency (USTDA) has continuously improved and enhanced the security of its information services. USTDA increased the number of IT policies mapped to NIST 800-53 standards from eight in FY 2018, to eighteen in FY 2019. Further, USTDA has implemented the TIC with an MOU in place with DHS. USTDA has secured additional resources and tools to be implemented that would allow USTDA to have a stronger security posture. In 2018 USTDA moved their external website to be hosted under MAX.gov to ensure stronger security and adherence to ongoing federal guidance.

### Independent Assessment

Identify - Overall considered effective but there are POA&Ms in each control family. The overall rating of defined or consistently implemented is primarily due to finalizing policies and related documents while procedures are currently in place and in varying states of implementation.

Protect - Overall considered effective but there are POA&Ms noted in control families. The overall rating of defined is primarily due to drafted policies and procedures being finalized while procedures are currently in place and in varying states of implementation.

Detect - The overall rating of Ad Hoc is primarily due to finalizing policies and related documents while procedures are currently in place and in varying states of implementation.

Respond - The overall rating of consistently implemented is primarily due to pending migration to Einstein.

Recover - The overall rating of consistently implemented is primarily due to implementing supply chain risks and metrics on effectiveness.

The independent review resulted in 35 remediation items included in the POA&Ms for the agency. Based on responses to the IG FISMA metrics and processes and procedures in place, the USTDA Information Security Program is effective.

# FY2019 Annual Cybersecurity Performance Summary

## United States AbilityOne Commission

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Consistently Implemented	Attrition	0	0	0
Protect	Managing Risk	Consistently Implemented	E-mail	0	0	0
Detect	Managing Risk	Defined	External/Removable Media	0	0	0
Respond		Consistently Implemented	Impersonation	NA	0	0
Recover	At Risk	Consistently Implemented	Improper Usage	0	0	0
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	1
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>1</b>

### CIO Self-Assessment

Evaluation of the FISMA CIO 2019 Q4/Annual assessment results revealed three High Risk findings due to protection controls not being implemented.

(1) Mobile device scanning- Mobile devices such as the Tablets and Laptops are not capable of scanning the device prior to remotely connecting to the commission network to prevent introducing any potential Malware or Malicious Code threat;

(2) High Value Asset (HVA) alternative site- U.S. AbilityOne systems are categorized under DHS guidance as HVA system because its requirement to its stored data; therefore, the system required to have an alternative offsite location to operate as a contingency location if disruption is more than 30 days;

(3) Remote Disk Wipe- The commission mobile devices (tablets and laptops) don't have the technology installed to remotely disk wipe the device hard-drive in the event of theft.

The commission is exploring/testing software solutions to remediate the remote disk wipe devices and to enable anti-virus scanning before devices connect to the network. Cost and feasibility analysis is underway to identify a viable off-site contingency solution, such as a FedRAMP approved Cloud Service Provider (CSP).

### Independent Assessment

Pursuant to the FY 2019 Inspector General FISMA Reporting Metrics, IGs are required to assess the effectiveness of information security programs on a maturity model spectrum. The guidance provides that in context of the maturity model, a Level 4 - Managed and Measurable, is defined as effective level for the information security program of an agency. The overall assessment of the Commission's information security program was deemed not effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating at Level 3 - Consistently Implemented.

# FY2019 Annual Cybersecurity Performance Summary

## United States Access Board

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Ad Hoc	Impersonation	NA	0	0
Recover	Managing Risk	Ad Hoc	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
<b>Overall</b>	<b>At Risk</b>		<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

The United States Access Board (USAB) conducted a risk assessment of its information and information systems. This assessment included risks to the agency's assets, mission essential functions, and level and program specific security reviews. USAB evaluated three elements from the master risk list to include: risk probability, impact and exposure. First, USAB assessed the likelihood of risk occurrence to the agency. Then, USAB inventoried the IT systems and data to create an individualized list of the risks impact to each system. Lastly, USAB performed a risk analysis of each system to identify vulnerabilities for management to develop a risk mitigation strategy. This approach allowed USAB operations staff and contractors to prioritize and effectively manage risks. USAB POA&M is the next step in the risk management process. USAB planning activities are carried out by its IT security and operations teams. The teams prioritize the risks and develop detailed strategies to address them. USAB POA&Ms includes scheduling the integration of the tasks required to implement the risk action plans into day-to-day operations activities by assigning them to individuals or roles and actively tracking the status. USAB management will use the Framework for Improving Critical Infrastructure Cybersecurity developed by NIST to manage the agency's cybersecurity risk. The agency had provided the semi-annual to the Secretary of DHS within the timeframe outlined. USAB systems had gone through the ATO process, and will be going through another Security Authorization and Assessment (SA&A) process in the next 3-5 months. Further, USAB is working with DHS through the CDM program and obtained shared services to mitigate and help improve the security posture of the organization.

### Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the United States Access Board was not performed for FY 2019, 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 USAB will explore contracting with an independent assessor in FY 2020.

# FY2019 Annual Cybersecurity Performance Summary

## United States Agency for Global Media

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Defined	Attrition	0	0	0
Protect	At Risk	Defined	E-mail	0	2	2
Detect	Managing Risk	Ad Hoc	External/Removable Media	0	0	0
Respond		Defined	Impersonation	NA	0	0
Recover	At Risk	Ad Hoc	Improper Usage	0	1	1
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	5	0	0
			Other	7	2	5
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>12</b>	<b>5</b>	<b>8</b>

### CIO Self-Assessment

Over the past year, U.S. Agency for Global Media (USAGM) has made significant progress in information security and risk management. Notable accomplishments include developing and beginning to implement a corrective action Plan to improve our information security program, publishing 21 information security policies, producing the Agency's first risk profile, and beginning to implement an information security RMF.

### Independent Assessment

Acting on behalf of the Office of IG, an independent public accounting firm conducted an audit to determine the effectiveness of USAGM's information security program and practices in accordance with FISMA requirements in FY 2019. The independent auditor concluded that USAGM does not have an effective organization-wide information security program for several reasons. OIG made two recommendations to improve USAGM's information security program.

# FY2019 Annual Cybersecurity Performance Summary

United States Agency for International Development (USAID)

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	Managing Risk	Managed and Measurable	Attrition	1	0	0
Protect	Managing Risk	Defined	E-mail	7	2	6
Detect	Managing Risk	Managed and Measurable	External/Removable Media	0	0	3
Respond		Managed and Measurable	Impersonation	NA	2	0
Recover	Managing Risk	Consistently Implemented	Improper Usage	10	15	22
<b>Overall</b>	<b>Managing Risk</b>		Loss or Theft of Equipment	30	9	3
			Web	21	8	24
			Other	123	20	103
			Multiple Attack Vectors	0	0	1
			<b>Total</b>	<b>192</b>	<b>56</b>	<b>162</b>

## CIO Self-Assessment

USAID's implementation of Emergency Directive (ED) 19-01 addressed the significant and imminent risks posed by illegitimate Domain Name Server (DNS) activity related to unauthorized certificates and provided the Agency with the strongest possible email authentication and web security protection.

To be vigilant, USAID conducted regular internal vulnerability assessments and quarterly independent penetration tests and established a follow-up plan to mitigate the security weaknesses that were identified.

Finally, the Agency's deployment of complementary cybersecurity tools strengthened its security posture by detecting and preventing malicious malware attacks, phishing emails, and unauthorized data ex-filtration, including threats to personally identifiable information (PII) and Advanced Persistent Threat (APT).

## Independent Assessment

USAID's information security program was evaluated as part of the FY 2019 FISMA Audit. This audit included an evaluation of 6 out of 45 FISMA reportable systems at USAID. A control was counted for each system it was tested against. Thus, there were 157 instances of testing a control. The FY 2019 FISMA Audit noted 144 instances of 157 selected NIST SP 800-53, Revision 4 security controls were 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.

# FY2019 Annual Cybersecurity Performance Summary

## United States Interagency Council on Homelessness

Framework	CIO Rating	IG Rating	Incidents by Attack Vector	FY17	FY18	FY19
Identify	At Risk	Ad Hoc	Attrition	0	0	0
Protect	At Risk	Ad Hoc	E-mail	0	0	0
Detect	At Risk	Ad Hoc	External/Removable Media	0	0	0
Respond	Managing Risk	Ad Hoc	Impersonation	NA	0	0
Recover		Ad Hoc	Improper Usage	0	0	0
<b>Overall</b>	<b>At Risk</b>		Loss or Theft of Equipment	0	0	0
			Web	0	0	0
			Other	0	0	0
			Multiple Attack Vectors	0	0	0
			<b>Total</b>	<b>0</b>	<b>0</b>	<b>0</b>

### CIO Self-Assessment

Per SP 800-60, Table 1: FIPS 199 Categorization, the United States Interagency Council for Homelessness' (USICH) sole information system is categorized as Low Impact. For FY 2019, USICH continued to update its SSP, and it will be updated periodically to incorporate new and/or modified security controls. USICH also changed IT service providers. Its new provider is supporting its FISMA and other IT/cybersecurity requirements. USICH's SSP 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 USICH was not performed for FY 2019, and the IG assessment section was marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the IG Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. USICH will explore contracting with an independent assessor in FY 2020.