Federal Information Security Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2017

The Office of Management and Budget (OMB) is publishing this report in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, § 3553 (Dec. 18, 2014) (codified at 44 U.S.C. § 3553). This report also incorporates the OMB's analysis of agency application of the intrusion detection and prevention capabilities, as required by Section 226 of the Cybersecurity Act of 2015 (Pub. L. No. 114-113). OMB obtained information from the Department of Homeland Security (DHS), and Chief Information Officers and Inspectors General from across the Executive Branch to compile this report. This report primarily includes Fiscal Year 2017 data reported by agencies to OMB and DHS on or before October 31, 2017.

Table of Contents

Executive Summary:
The State of Federal Cybersecurity

The far-reaching cybersecurity incidents of 2017 demonstrate that we cannot ignore the harmful impact that poor cybersecurity practices have on the Nation. Hundreds of millions of Americans had their personally identifiable information (PII) compromised in a string of data breaches that exploited unpatched vulnerabilities at companies whose core services focus on safeguarding that very information. Tens of thousands of Federal employees and taxpayers also had their information compromised because of agencies' limited data and website protections. These incidents continue to demonstrate that effective cybersecurity requires any organization — whether a Federal agency or a public or private company — to identify, prioritize, and manage cyber risks across its enterprise.

In this spirit, the President signed Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* (Executive Order No. 13800) in May 2017 to enhance cybersecurity risk management across the Federal Government. Executive Order 13800 recognizes that the Government must ensure that it can secure citizens' information and that agencies can deliver on their core missions and services even as malicious cyber actors seek to disrupt those services. Accordingly, Executive Order 13800 required every agency to conduct comprehensive reviews of their cybersecurity programs, and for the Office of Management and Budget (OMB), Department of Homeland Security (DHS), Department of Defense, and several other key agencies to review cybersecurity practices across the Government and the critical infrastructure sectors.

While the Executive Order is the catalyst for securely modernizing Federal IT systems over the coming years, OMB and DHS's long-running efforts to instill disciplined cyber practices across government helped safeguard agency IT systems in 2017. As a clear example, DHS's efforts ensured that Federal agencies had already patched their systems to protect against the vulnerability that led to the WannaCry, Petya, and NotPetya ransomware before those attacks swept across the globe. Agencies also expanded their use of continuous monitoring tools and of multi-factor authentication Personal Identity Verification (PIV) cards throughout the year.

Although this progress is encouraging, agencies endured 35,277 cybersecurity incidents in Fiscal Year (FY) 2017, which is a 14% increase over the 30,899 incidents that agencies reported in FY 2016, with five of the FY 2017 incidents reaching the threshold of "major incident" due to their impact. OMB, DHS, and agency partners must continue to act to reduce the disruption that cybersecurity incidents have on the Federal enterprise. Accordingly, this annual FISMA report to Congress highlights government-wide programs and initiatives as well as agencies' progress to enhance Federal cybersecurity over the past year and into the future.

A. Federal Cybersecurity Roles and Responsibilities

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

Office of Management and Budget (OMB): OMB is responsible for overseeing Federal agencies' information security and privacy practices and for developing and implementing related policies and guidelines. The Federal Chief Information Security Officer leads the OMB Cyber and National Security Unit, which serves as the dedicated team within the Office of Electronic Government (Office of the Federal Chief Information Officer (OFCIO)) that works with Federal agency leadership to address information security priorities. The OMB Cyber and National Security Unit collaborates with partners across the government to develop cybersecurity policies, conduct data-driven oversight of agency cybersecurity programs, and coordinate the Federal response to cyber incidents. The Office of Information and Regulatory Affairs is responsible for providing assistance to Federal agencies on privacy matters, developing Federal privacy policy, and overseeing implementation of privacy policy by Federal agencies.

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

Department of Homeland Security (DHS): DHS is the operational lead for Federal cybersecurity and has the authority to coordinate government-wide cybersecurity efforts, issue binding operational directives (BODs) detailing actions that agencies should take to improve their cybersecurity, and provide operational and technical assistance to agencies, including through the operation of the Federal information security incident center. Under FISMA and other authorities, DHS provides common security capabilities for agencies through the National Cybersecurity Protection System (which includes the EINSTEIN program) and Continuous Diagnostics and Mitigation (CDM) program and provides incident response assistance through the National Cybersecurity and Communications Integration Center (NCCIC) in accordance with Presidential Policy Directive-41, United States Cyber Incident Coordination. DHS also facilitates information sharing across the Federal Government and the private sector.

General Services Administration (GSA): GSA provides management and administrative support to the entire Federal Government and establishes acquisition vehicles for agencies' use. This includes the recently established Centers of Excellence, which provide expert advice, consulting, development and support solution

implementation in the areas of: Cloud Adoption; IT Infrastructure Optimization; Customer Experience; Service Delivery Analytics; and Contact Centers. GSA also hosts the Federal Risk and Authorization Management Program (FedRAMP), which promotes the use of secure cloud-based services in government.

National Institute of Standards and Technology (NIST): NIST, a bureau of the Department of Commerce, is charged with developing standards and guidelines for Federal information systems, in coordination with OMB and other Federal agencies. Among other roles, NIST creates Federal Information Processing Standards (FIPS) and provides management, operational, and technical security guidelines on a broad range of topics, including incident handling and intrusion detection, supply chain risk management, and strong authentication. Additionally, NIST develops and updates the Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

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

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

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

Section I: Federal Cybersecurity at a Glance

A. Federal Cybersecurity Year in Review

The President has made strengthening the Nation's cybersecurity a priority from the outset of this Administration. In May 2017, the President signed Executive Order No. 13794, *Establishment of the American Technology Council*, which promotes the secure and efficient use of Information Technology (IT), and Executive Order 13800, which concentrates on IT modernization and cybersecurity risk management. Executive Order 13800 reinforces FISMA by holding agency heads accountable for managing cybersecurity risks to their enterprises.[1] Executive Order 13800 also requires each agency to assess its cybersecurity risks and submit a plan to OMB for implementing the NIST Cybersecurity Framework.[2]

The White House published the *Report to the President on Federal IT Modernization*,[3] as part of the Executive Order 13800 implementation effort. The report details activities to modernize and safeguard high-risk High Value Assets (HVAs), promotes the consolidation of network acquisitions and management, and prompts agencies to leverage commercial cloud solutions and cybersecurity shared services where available. Additionally, OMB developed the *Federal Cybersecurity Risk Determination Report and Action Plan*, which assesses the sufficiency of agencies' risk mitigation and acceptance choices and includes a plan for remediating gaps. OMB reviewed 97 agency risk management assessments and found that agencies lack situational awareness of the threat environment, capabilities to detect intrusions and data exfiltration, and fundamental accountability for mitigating cyber risks across the enterprise.

During the year, OMB and DHS continued their work with the CIO and Inspectors General (IG) communities to align program oversight practices and FISMA metrics with the NIST Cybersecurity Framework's five function areas of Identify, Protect, Detect, Respond, and Recover. OMB also enhanced the IT Security portion of Capital Planning and Investment Control guidance in OMB Circular A-11.[4] This alignment has helped to standardize and define common vocabulary used in security, mirroring the

---

[1] 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 (i) information collected or maintained by or on behalf of [an] agency and (ii) 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.

[2] 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

[3] American Technology Council, Report to the President on Federal IT Modernization (2017), https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf).

[4] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-11, Preparation, Submission, and Execution of the Budget (July 1, 2016).

standardization that is increasingly necessary and useful with private sector suppliers, vendors, and industry partners.

B. FY 2017 Policy Updates

High Value Assets (HVAs)

In early FY 2017, OMB emphasized the importance of the HVA effort by establishing guidance for agencies to engage in the ongoing identification, categorization, prioritization, reporting, assessment, and remediation of HVAs in OMB Memorandum M-17-09, *Management of Federal High Value Assets*.[5] The Memorandum directs all agencies to review all critical assets, systems, information, and data continuously in order to understand the potential impact of a cyber-incident on those assets and to ensure that robust physical and cybersecurity protections are in place. The *Report to the President on Federal IT Modernization* also outlines steps to enhance oversight of the HVA Program, including revising NIST's Federal Information Processing Standard (FIPS) Publications 140-2,[6] 199,[7] and 200,[8] updating the annual FISMA CIO metrics to track controls for HVAs, and developing a playbook for agencies as they manage their systems in a prioritized, risk-based approach.

Personally Identifiable Information (PII) Breach Preparation and Response

OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*,[9] released in January 2017, updates existing OMB breach notification policies and guidelines in accordance with FISMA and implements recommendations from OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*.[10] Among other items, the policy requires that each agency's Senior Agency Official for Privacy (SAOP) develop and implement a breach response plan and incorporate the plan into the agency's formal incident response plan. The policy also outlines a series of elements that each agency must incorporate into its breach response plan.

---

[5] Office of Mgmt. & Budget, Exec. Office of the President, M-17-09, Management of Federal High Value Assets (2016).
[6] Nat'l Inst. of Standards & Tech., FIPS PUB 140-2, Security Requirements for Cryptographic Modules (2001).
[7] Nat'l Inst. of Standards & Tech., FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (2004).
[8] Nat'l Inst. of Standards & Tech., FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems (2006).
[9] Office of Mgmt. & Budget, Exec. Office of the President, M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017) [hereinafter OMB Memorandum M-17-12].
[10] Office of Mgmt. & Budget, Exec. Office of the President, M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct. 30, 2015).

C. Initiatives to Enhance Federal Cybersecurity Oversight

Continuous Diagnostics and Mitigation (CDM)

A lack of visibility into an agency's internal IT environment increases the risk that unauthorized activities are taking place facilitated by the use of unregistered hardware or software. The CDM program exists to reduce this risk by helping agencies understand and monitor their environments. Nearly 20 agencies now report data in near-real-time to their own dashboards after deploying CDM Phase 1 sensors and tools. Agencies participating in Phase 1 also have automated vulnerability patching to significantly reduce threat-exposure windows and an active hunt capability using real-time endpoint queries to enable targeted malware searches.

During FY 2017, CDM began deploying Phase 2 tools and sensors that support agencies in better managing both privileged and general users. Additionally, the program continued to build out the shared services platform through which CDM will deliver Phase 1 and 2 tools to non-CFO Act agencies, providing much-needed network security capabilities at a sustainable cost. In tandem, the CDM program began working on a risk scoring approach that incorporates DHS threat intelligence data, called Agency-wide Adaptive Risk Enumeration. The Agency-wide Adaptive Risk Enumeration will allow prioritization of mitigation activities using threat data combined with agency dashboard data regarding the existence of known vulnerabilities and the FIPS 199 information system impact level (high, moderate, or low). Agencies will be able to use this risk scoring approach to improve cybersecurity hygiene.

In FY 2018, the CDM program office will continue to incorporate additional capabilities, including CDM Phase 3. Agencies will also begin sending summary feeds to the Federal Dashboard, which, upon launch, will enable an enterprise-wide view of the government's cybersecurity posture.

National Cybersecurity Protection System (including EINSTEIN)

EINSTEIN is a key component of the National Cybersecurity Protection System, which provides a suite of tools designed 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, analysis, and information sharing system that builds on the passive detection capabilities of EINSTEIN 1 and EINSTEIN 2. The E3A program also serves as a platform to aggregate Federal civilian executive branch traffic so that DHS can implement new and advanced protections. As of September 29, 2017, DHS reports that, of 119 Federal civilian agencies, 31 report implementing all three NCPS capabilities, 17 of which are CFO Act agencies.

Table 1: NCPS Intrusion Detection and Prevention Capabilities Implementation Summary for Federal Civilian Agencies [11]

Capability	Complete	In Progress	Deferred[12]	Not Implemented
E1/E2	**75** (63%)	**2** (2%)	**0** (0%)	**42** (35%)
CFO Act[13] Only	*21 (91%)*	*2 (9%)*	*0 (0%)*	*0 (0%)*
E^{3}A (DNS Sinkholing)	**72** (61%)	**12** (10%)	**0** (0%)	**35** (29%)
CFO Act Only	*23 (100%)*	*0 (0%)*	*0 (0%)*	*0 (0%)*
E^{3}A (Email Filtering)	**39** (33%)	**14** (12%)	**16** (13%)	**50** (42%)
CFO Act Only	*15 (65%)*	*6 (26%)*	*2 (9%)*	*0 (0%)*

DHS reports that between January 1, 2016 and April 28, 2017, key indicators for NCPS include detecting 1,600 incidents across Federal civilian networks via its E1 and E2 capabilities, and detecting and preventing 633 incidents via E3A DNS Sinkholing and Email Filtering capabilities.

High Value Asset (HVA) Program

OMB and DHS developed the HVA program in 2015 to safeguard critical information systems and assets across the Federal enterprise. OMB establishes the policy direction for the program and DHS manages the operational program management office that assists agencies with mitigating cybersecurity risks. The primary HVA services are:

- *Security Architecture Review (SAR)* – an in-depth, non-intrusive analysis of the security control selection, application and effectiveness for a given system or enterprise.
- *Risk and Vulnerability Assessment (RVA*) – a penetration test based assessment utilizing scenarios by adversaries to compromise data, networks, and systems.

In FY 2017, the DHS HVA Program conducted 13 SARs and 20 RVAs. These assessments revealed that the Federal Government's continued challenges mitigating basic security vulnerabilities. The most common security vulnerabilities identified across the HVA landscape were: 1) lack of strong authentication, 2) lack of network segmentation, 3) inconsistent patch management, 4) spear phishing, and 5) gaps in security capabilities and protections.

11 This table provides implementation status based on the lowest implementation status of all of an agency's components.
12 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.
13 Civilian CFO Act Agencies pursuant to 31 U.S.C. § 901 (a)-(b).

Top Five FY 2017 SAR Findings

- Lack of Strong Authentication
- Lack of Network Segmentation
- Security Capabilities and Protection Gaps
- Asset Management and Network Access Control
- Data Protection

Top Five FY 2017 RVA Findings

- Spear Phishing Weaknesses
- Patch Management
- Sensitive Data Exfiltration
- Cleartext Password Disclosure
- Easily Guessable Credentials

DHS also provides scanning and testing services through its National Cybersecurity Assessment and Technical Services (NCATS) team, based out of the National Cybersecurity and Communications Integration Center. In FY 2017, the NCATS team received 151 requests for penetration tests from Federal agencies and was able to perform only 71 due to resource constraints. The top findings of these tests are consistent with the FY 2017 SAR and RVA findings, underscoring the need for agencies to prioritize protection of the nation's most critical IT systems.

Automated Indicator Sharing (AIS)

The AIS capability enables the exchange of cybersecurity threat indicators between the Federal Government and the private sector at machine speed. Indicator information that is shared includes malicious internet protocol addresses and the sender address of phishing emails. Ultimately, the goal is to commoditize cybersecurity threat indicators through AIS so that tactical indicators are shared broadly among the public and private sector, enabling everyone to be better protected against cybersecurity attacks. Twenty-three (23) CFO Act agencies and eight non-CFO Act agencies have signed Multilateral Information Sharing Agreements and are receiving indicators as of the end of FY 2017. Twelve CFO Act agencies are utilizing direct connections, eight utilize shared service connections, and three utilize both connection types. Since AIS's inception in March 2016, DHS has shared more than 1.6 million unique threat indicators throughout the AIS ecosystem. Several Federal and non-Federal partners are also submitting information to DHS through AIS. In total, DHS has received over 900,000 indicators from Federal partners and the private sector.

Binding Operational Directives (BODs)

DHS has the authority to issue compulsory directions to Federal agencies known as Binding Operational Directives (BODs) in accordance with FISMA.[14] In line with OMB's policies, principles, standards, and guidelines, BODs seek to safeguard Federal information and information systems from known or reasonably suspected information

[14] 44 U.S.C. §§ 3552(b)(1), 3553(b)(2).

security threats, vulnerabilities, or risks. The National Protection and Programs Directorate Federal Network Resilience Division leads DHS efforts to communicate and manage actions and critical activities related to all BODs. Since acquiring this authority, DHS has issued five BODs to address vulnerabilities impacting Federal agencies, including one in FY 2017.

- ***BOD 17-01: Removal of Kaspersky-Branded Products***: DHS, after consulting with NIST and coordinating with other interagency partners, determined that Kaspersky-branded products present a known or reasonably suspected information security risk to Federal information systems. BOD 17-01 requires agencies to identify the presence of any Kaspersky Lab products on their Federal information systems within 30 days of BOD issuance, develop a plan to remove and discontinue use of such products within 60 days of BOD issuance, and, unless directed otherwise by DHS based on new information, start removing those products from agency networks on December 12, 2017 (90 days after BOD issuance).

D. IT Security Spending Reported by CFO Act Agencies

The FY 2017 spending data shows over $5.6 billion in civilian agency cybersecurity spending, including spending on cybersecurity related mission activities, as detailed in Table 2.

Table 2: FY 2017 Civilian CFO Agency Cybersecurity Spending

Agency	FY 2017 Spending ($ in Millions)	Agency	FY 2017 Spending ($ in Millions)
Commerce	$273.77	NASA	$148.42
DHS	$1,614.28	NRC	$22.68
DOT	$140.15	NSF	$182.74
ED	$74.11	OPM	$37.56
Energy	$370.61	SBA	$19.50
EPA	$25.14	SSA	$156.28
GSA	$65.87	State	$254.30
HHS	$319.66	Treasury	$458.35
HUD	$15.22	USAID	$36.48
Interior	$84.04	USDA	$114.65
Justice	$735.03	VA	$385.81
Labor	$83.41	**Total**	**$5,618.04**

The Federal Government continues to improve its overall cybersecurity posture. In order for agencies to make risk-informed budget decisions, they must have a better understanding of how each incremental dollar reduces risk to their agency. Accordingly, OMB recently developed reporting structures to capture agency spending and budget information at the cybersecurity capability level. OMB will work with agencies throughout FY 2018 to integrate these structures into strategic planning and risk management discussions with agency CIOs, CISOs, and CFOs.

Section II: Senior Agency Official for Privacy (SAOP) Performance Measures

In today's digital world, effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards, commonly referred to as "controls," employed within the information systems that process, store, and transmit the information. As such, Federal agencies are required to develop, implement, and maintain agency-wide privacy programs that among other things, where PII is involved, play a key role in information security and implementing the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF).[15]

Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, recognizes that effective risk management requires agency heads to lead integrated teams of senior executives, including executives with expertise in privacy. While the head of each Federal agency remains ultimately responsible for ensuring that privacy interests are protected and that PII is managed responsibly within their respective agency, Executive Order No. 13719, *Establishment of the Federal Privacy Council*, requires agency heads to designate or re-designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for the agency's privacy program. In accordance with OMB Circular A-130, the SAOP is responsible for reviewing and approving, in accordance with standards promulgated under section 11331 of title 40, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. OMB Circular A-130 provides additionally that the SAOP reviews the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization by the agency CIO. Privacy plans detail the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, detail how the controls have been implemented, and describe the methodologies and metrics that will be used to assess the controls.[16]

For FY 2017, all 24 CFO Act agencies and 57 non-CFO Act agencies reported SAOP FISMA performance measures to OMB. OMB significantly modified the SAOP FISMA performance measures for FY 2017 to account for several major privacy-related policies that were either issued or reissued in FY 2016 or at the start of FY 2017. These policies

[15] 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].
[16] *See id*.

include OMB Circular A-130,[17] *Managing Information as a Strategic Resource*, OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, [18] OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*,[19] and OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*.[20]

A. Privacy Programs and the NIST Risk Management Framework

Federal agencies are required to develop, implement, document, maintain, and oversee agency-wide privacy programs that include people, processes, and technologies. Agencies' privacy programs are responsible for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risk.

In order to effectively manage privacy risk, Federal privacy programs have specific responsibilities under the NIST RMF. The NIST RMF is a disciplined and structured process that agencies are required 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 3: General Privacy Program Requirements

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Has the head of the agency designated an SAOP?[21]	100%	96%
Does the SAOP have the necessary role in the agency's policy making, compliance, and risk management activities?[22]	96%	96%
Does the agency identify and plan for the resources needed to implement the agency's privacy program?[23]	83%	86%

[17] *See id*.
[18] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act (Dec. 23, 2016) [hereinafter OMB Circular A-108].
[19] Office of Mgmt. & Budget, Exec. Office of the President, M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016) [hereinafter OMB Memorandum M-16-24].
[20] Office of Mgmt. & Budget, Exec. Office of the President, M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (2017) [hereinafter OMB Memorandum M-17-12].
[21] *See* OMB Memorandum M-16-24, *supra* note 5.
[22] *See id*.
[23] *See* OMB Circular A-130, *supra* note 1, at § 4(b)(1).

Has the agency developed and maintained a privacy program plan?[24]	92%	79%

Table 4: Privacy and the NIST Risk Management Framework

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Has the agency implemented a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems?[25]	92%	68%
Does the SAOP review and approve, in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[26]	83%	77%
Has the SAOP designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency?[27]	83%	46%
Has the agency developed and maintained a privacy plan, reviewed and approved by the SAOP, for agency information systems prior to authorization, reauthorization, or ongoing authorization?[28]	75%	58%

[24] 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, *supra* note 1, at app. I §§ 4(c)(2), 4(e)(1).
[25] *See* OMB Circular A-130, *supra* note 181, at app. I §§ 3(a), 3(b)(5).
[26] *See id.* at App. I §§ 4(a)(2), 4(e)(7).
[27] *See id.* at App. I §§ 4(e)(5), 10(a)(14), 10(a)(26), 10(a)(66) and 10(a)(86).
[28] 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, *supra* note 181, at app. I §§ 4(c)(9), (e)(8).

Does the SAOP conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks?[29]	75%	53%
Has the SAOP developed and maintained a written privacy continuous monitoring strategy?[30]	71%	46%
Has the SAOP established and maintained an agency-wide privacy continuous monitoring program?[31]	63%	42%
Does the SAOP review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions?[32]	83%	72%

B. Information Systems and Personally Identifiable Information

The Federal Government necessarily creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of PII to carry out missions mandated by Federal statute. Agencies are required to monitor and assess security and privacy controls selected for information systems and must continue to monitor and assess those controls on an ongoing basis. This includes assessing the effectiveness of the security and privacy controls, documenting changes to the information system, analyzing the security and privacy impact associated with the changes, and reporting the state of the system to appropriate agency officials. Federal agencies' privacy programs are required to maintain an inventory of information systems that create,

[29] *See id.* at App. I § 4(3).
[30] The SAOP is required to develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. *See* OMB Circular A-130, *supra* note 181, at app. I §§ 4(d)(9), 4(e)(2).
[31] The SAOP is required to establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. *See id.* at app. I §§ 4(d)(10)–(11), 4(e)(2).
[32] *See id*. at app. I § 4(e)(9).

collect, use, process, store, maintain, disseminate, disclose, or dispose of PII. Maintaining such an inventory allows privacy programs to maintain an ongoing awareness of their PII holdings and to effectively monitor and assess the privacy controls selected for those information systems.

Table 5: Information Systems and Personally Identifiable Information

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency maintain an inventory of the agency's information systems[33] that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[34]	96%	90%
Does the agency ensure, to the extent reasonably practicable, that PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of is accurate, relevant, timely, and complete?	96%	97%
Does the agency limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions?	96%	98%
Does the agency ensure that, in a timely manner, the SAOP is made aware of information systems and components that cannot be appropriately protected or secured?[35]	88%	91%
Number of reported information systems that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[36]	4,555	780

[33] 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* § 3502(8) (2012). 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 *supra* note 1, at § 10(a)(23).

[34] *See* OMB Circular A-130, *supra* note 1, at §§ 5(a)(1)(a)(ii), 5(f)(1)(e).

[35] *See id*. at Appendix I § 3(b)(10).

[36] 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, *supra* note 1, at, app. II § 4(j)(2)(c).

In addition to managing the privacy risks associated with PII generally, Federal agencies are required to take additional steps to manage the risk associated with the collection, maintenance, and use of Social Security numbers (SSNs). The Federal Government uses SSNs as unique identifiers for many purposes, including employment, taxation, law enforcement, and benefits. However, SSNs are also key pieces of identifying information that potentially may be used to perpetrate identity theft. As such, Federal agencies are required to eliminate the unnecessary collection, maintenance, and use of SSNs, and explore alternatives to the use of SSNs as a personal identifier.

Table 6: Elimination of the Unnecessary Use and Collection of Social Security Numbers (SSNs)

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency have an inventory of the agency's collection and use of SSNs?[37]	88%	75%
If the agency does have an inventory of its collection and use of SSNs, does the agency maintain the inventory of SSNs as part of the agency's inventory of information systems?	81%	79%
Has the agency developed and implemented a written policy or procedure to ensure that any new collection or use of SSNs is necessary?	96%	67%
If the agency has not successfully eliminated all unnecessary collections and uses of SSNs at the agency, did the agency take steps during the reporting period to eliminate the unnecessary collection and use of SSNs?[38]	96%	85%

C. Privacy Risk and IT Development and Investment

Effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their PII requires that Federal privacy programs consider the potential impact on individuals' privacy throughout the system development lifecycle.[39] Federal agencies are required

[37] 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.
[38] *See* OMB Circular A-130, *supra* note 1, at § 5(f)(1)(f).
[39] *See* OMB Circular A-130, *supra* note 1, at § 5(a)(1)(c)(i).

to consider privacy when analyzing IT investments, and are required establish a decision-making process that covers the life of each information system and includes explicit criteria for analyzing the projected and actual costs, benefits, and risks, including privacy risks, associated with the IT investments.[40]

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.[41] A PIA is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. SAOPs work closely with the program managers, information system owners, information technology experts, security officials, counsel, and other relevant agency officials in order to conduct a meaningful assessment.

Table 7: Developing and Procuring Information Technology

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency have a process that includes explicit criteria for analyzing privacy risks when considering IT investments?[42]	75%	53%
During the reporting period, did the agency review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, were explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[43]	75%	61%

[40] *See* OMB Circular A-130, *supra* note 1, at § 5(d)(3).

[41] *See* 44 U.S.C. § 3501 note (Federal Management and Promotion of Electronic Government Services); *accord* Pub. L. 107–347, § 208(b). Section 208(b) of the E-Government Act requires agencies, absent an applicable exception under this section, to conduct a PIA before: (i) developing or procuring IT that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that – (I) will be collected, maintained, or disseminated using IT; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

[42] *See id*. OMB Circular A-130, *supra* note 1, at § 5(d)(3).

[43] *See id*. at § 5(a)(3)(e)(ii).

Does the agency plan and budget to upgrade, replace, or retire any information systems that maintain PII for which protections commensurate with risk cannot be effectively implemented?[44]	88%	74%
Does the agency ensure that, in a timely manner, the SAOP is made aware of information systems and components that cannot be appropriately protected or secured?[45]	88%	91%

Table 8: Policies and Procedures for Privacy Impact Assessments

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Has the agency developed and implemented a written policy or procedure for determining whether a PIA is required when the agency develops, procures, or uses an IT system?[46]	96%	74%
Has the agency developed and implemented a written policy or procedure to ensure that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks?[47]	96%	68%

Table 9: Privacy Impact Assessments

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Number of information technology (IT)[48] systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) for which the agency is required to conduct a privacy impact assessment (PIA).	3,275	878

[44] *See id*. at Appendix I § 4(b)(3).
[45] *See id*. at Appendix I § 3(b)(10).
[46] *See id*. at Appendix II § 5(e).
[47] *See* OMB Circular A-130, *supra* note 1 at app. II § 5(e).
[48] The term "information technology" means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. *See* Office of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003).

Number of reported IT systems that are covered by an up-to-date PIA.[49]	2,747	716
Percentage of IT systems with an up-to-date PIA.	***84%***	***82%***

D. Administrative, Technical, and Physical Safeguards for Systems of Records

Among other things, the Privacy Act of 1974 requires agencies to establish reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access and otherwise to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Privacy Act requirements are integral to protecting Federal information and information systems. Implementation of the Privacy Act directly affects the ability of agencies to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of certain information about individuals maintained by Federal agencies and to protect Federal information and information systems as required by FISMA.

Table 10: Administrative, Technical, and Physical Safeguards for Systems of Records

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that no system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order?[50]	92%	67%
Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to	92%	59%

[49] 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, *supra* note 1 at app. II § 5(e).

[50] *See* OMB Circular A-108, *supra* note 4, at § 12(a); see also 5 U.S.C. § 552a(e)(1).

ensure that all SORNs remain accurate, up-to-date, and appropriately scoped; that all SORNs are published in the *Federal Register*; that all SORNs include the information required by OMB Circular A-108; and that all significant changes to SORNs have been reported to OMB and Congress?[51]		
Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that all routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected?[52]	92%	68%
Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that the language of each contract that involves the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals, is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees?[53]	92%	61%

E. 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 respective agency.

[51] *See* OMB Circular A-108, *supra* note 4, at § 12(b).
[52] *See id*. at § 12(c).
[53] *See id*. at § 12(e).

Table 11: Workforce Management

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency ensure that the agency's privacy workforce has the appropriate knowledge and skill?[54]	88%	87%
Is the SAOP involved in assessing the hiring, training, and professional development needs of the agency with respect to privacy?[55]	88%	80%

Table 12: Training and Accountability

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Has the agency developed, maintained, and implemented mandatory agency-wide privacy awareness and training programs for all employees?[56]	100%	88%
Has the agency provided role-based privacy training during the reporting period for employees and contractors with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties?[57]	83%	54%
Has the agency developed and implemented policies and procedures to ensure that all personnel are held accountable for complying with agency-wide privacy requirements and policies?[58]	92%	88%

F. Contractors and Third Parties

In addition to managing the risk to individuals when Federal agencies create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information, Federal privacy programs are also required to manage the associated privacy risk when other entities operate or use information systems on behalf of a Federal agency.

[54] *See* OMB Circular A-130, *supra* note 1, at § 5(c)(2).
[55] *See id*. at § 5(c)(6).
[56] *See id*. at Appendix I § 4(h)(1).
[57] *See id*. at Appendix I § 4(h)(5).
[58] *See id*. at Appendix I § 3(b)(9).

Table 13: Contractors and Third Parties

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency ensure that terms and conditions in contracts, and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal 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?[59]	96%	91%
Does the agency, consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function?[60]	96%	97%
Does the agency document and implement policies and procedures for privacy oversight of contractors and other entities, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information?[61]	96%	86%

G. Incident Response

Federal agencies' privacy programs and their respective SAOPs are required to take specific steps to prepare for and respond to a breach of PII.[62] 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.[63]

[59] *See id*. at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).
[60] *See id*. at Appendix I § 4(j)(3).
[61] *See id*. at Appendix I § 4(j)(2)(a).
[62] The term "breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. *See* OMB Memorandum M-17-12, *supra* note 6, at § VII.
[63] *See id*.

Table 14: Incident Response

FY 2017 – SAOP FISMA Performance Measures	CFO Act	Non-CFO Act
Does the agency have a breach response plan that includes the agency's policies and procedures for reporting, investigating, and managing a breach?[64]	100%	91%
If the agency has a breach response plan, did the SAOP review the agency's breach response plan during the reporting period to ensure that the plan is current, accurate, and that it reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology?[65]	100%	94%
Does the agency have 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?[66]	100%	83%
If the agency has a breach response team, did all members of the agency's breach response team participate in at least one tabletop exercise during the reporting period?[67]	67%	41%
How many breaches, as the term "breach" is defined in OMB Memorandum M-17-12, were reported within the agency during the reporting period?[68]	24,056	689
How many breaches did the agency's principal security operations center report to the DHS United States Computer Emergency Readiness Team (US-CERT) during the reporting period?[69]	6,213	262
How many breaches did the agency report to Congress during the reporting period?[70]	3,186	5

[64] *See id*. at § VII, XI.
[65] *See id*. at § X.B, XI.
[66] *See id*. at § VII.A, XI.
[67] *See id*. at § X.A, XI.
[68] *See id*. at § III.C, XI.
[69] *See id*. at § VII.D.1, XI. Note that while US-CERT captures breaches in its incident reporting, these 6,213 reflect breaches reported to US-CERT, and not breaches that are necessarily captured in the final incident count in section III.B of this report.
[70] *See id*. at § VII.D.3, XI.

What is the total number of individuals potentially affected by the breaches reported to Congress during the reporting period?[71]	25.5 M[72]	48,856

[71] *See id*. at § XI.

[72] There were 25,496,896 individuals potentially affected by the breaches CFO Act agencies reported to Congress in FY 2017. Of those individuals potentially affected, 25 million were reported by one Federal agency.

Section III: FY 2017 Agency Performance

A. Introduction to Agency Cybersecurity Performance Summaries

This year's report structure 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." Each agency narrative contains four sections: Risk Management Assessment, CIO Assessment, IG Assessment, and US-CERT Incidents. The Risk Management Assessments, new to this year's report, build upon the process established pursuant to Executive Order No. 13800. The metrics that inform these assessments reflect baseline security controls that all agencies must meet. The descriptions below provide an overview of the sections included in each agency performance summary.

Risk Management Assessments

Following the President's issuance of Executive Order No. 13800, OMB, in coordination with DHS, developed a process to evaluate the degree to which agencies manage their cybersecurity risk at the enterprise level. OMB released its methodology for this process as part of OMB Memorandum M-17-25, *Reporting Guidance for the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*,[73] which also described other requirements established under Executive Order No. 13800.

The risk assessments leverage the FY 2017 FISMA CIO metrics and IG metrics in domains that correspond with each of the five NIST Cybersecurity Framework function areas:

- **Identify** (Asset Management and Authorization; Comprehensive Risk Management)
- **Protect** (Remote Access Protection; Credentialing and Authorization; Network Protection)
- **Detect** (Anti-Phishing Capabilities; Malware Defense Capabilities; Exfiltration and Other Capabilities)
- **Respond** (Planning and Processes; Evaluation and Improvement)
- **Recover** (Planning and Testing; Personal Impact Process; Back-Up Capacity)

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.

[73] Office of Mgmt. & Budget, Exec. Office of the President, M-17-25, Reporting Guidance for the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 19, 2017).

- **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.

Chief Information Officer Assessment

The CIO narrative 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.

Inspector General Assessment[74]

The IG narrative section allows IGs and independent assessors to frame the scope of their analysis, identify key findings, and detail recommendations to address those findings. The IG assessment also captures the IG's maturity model ratings for the agency. In FY 2017, the IG community, in partnership with OMB and DHS, finalized a three-years-long effort to create maturity models for FISMA metrics that align to the five function areas in the NIST Cybersecurity Framework. This alignment helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes and provides agencies with a meaningful independent assessment of their information security programs. Table 15 details the five possible maturity levels that each of the NIST Cybersecurity Framework function areas could be assessed at for a given agency.

Table 15: IG Assessment Maturity Levels

Maturity Level	Maturity Level Distribution
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organizations and used to assess them and make necessary changes.
Level 5: Optimized	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.

[74] 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 narrative.

Table 16 provides the median maturity model ratings across the five NIST Cybersecurity Framework functions from 76 agency IG and independent auditor assessments. Per the FY 2017 IG FISMA Reporting Metrics , a finding of *Managed and Measureable* 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 2017 IG FISMA Metrics allowed individual IGs 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. As noted in the Government Accountability Office report Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices (GAO-17-549), OMB will continue to work with the IG community, as well as DHS and the CIO Council, to enhance the maturity model and its underlying methodology.

Table 16: Median Government-wide Maturity Model Ratings

NIST Cybersecurity Framework Area	Median Rating
Identify	**Level 3**: Consistently Implemented
Protect	**Level 3**: Consistently Implemented
Detect	**Level 2**: Defined
Respond	**Level 3**: Consistently Implemented
Recover	**Level 3**: Consistently Implemented

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

CAP Goals offer a mechanism for accelerating progress in priority areas where active collaboration between OMB and Federal agencies is required. Table 17 details agency progress towards meeting targets for the three FY 2015–2017 cybersecurity priority areas: Information Security Continuous Monitoring; Identity, Credential, and Access Management; and Anti-Phishing and Malware Defense.

Table 3: FY 2015 - FY 2017 CAP Goal Summary

CAP Goal Metric	Metric Target	Number of Agencies Meeting Target			Implementation Percentage Across All Agencies*		
		FY 2015	FY 2016	FY 2017	FY 2015	FY 2016	FY 2017
Information Security Continuous Monitoring (ISCM)							
Hardware Asset Management	95%	35	32	51	61%	61%	67%
Software Asset Management	95%	21	35	49	54%	61%	66%
Vulnerability Management	95%	28	60	73	70%	90%	95%
Secure Configuration Management	95%	39	62	76	91%	92%	95%
Identity, Credential, and Access Management (ICAM)							
Unprivileged User PIV Implementation	85%	27	40	48	62%	81%	85%
Privileged User PIV Implementation	100%	24	40	46	78%	89%	93%
Anti-Phishing and Malware Defense (APMD)							
Anti-Phishing Defenses	5 of 7	29	69	86	--	--	--
Malware Defenses	3 of 5	33	65	88	--	--	--
Other Defenses	2 of 4	51	77	88	--	--	--

*The percentages in the portion of this table labeled “ISCM” are calculations of the number of compliant assets across the government / total number of assets across the government. The percentages in the portion of this table labeled “ICAM” are calculations of the number of compliant users across the government / total number of users across the government. Analysis of FISMA Agency Level Questions Data (ISCM: Questions 1.2, 1.4, 1.5, 2.2, 2.3, 3.16, 3.17; ICAM: Questions 2.4, 2.5; APMD: Questions 2.19, 3.1-3.15), reported to DHS via CyberScope from October 1, 2015, to September 30, 2017. OMB used a weighted average of the total number of applicable assets to determine the government-wide average.

B. FY 2017 Information Security Incidents

US-CERT Incidents by Attack Vector

Agency incident data provides an indication of the threats agencies face every day and the persistence of those incidents. In accordance with FISMA, OMB provides summary information on the number of cybersecurity incidents that occurred across the Federal Government and at each Federal agency. The FY 2017 FISMA Report captures incidents in accordance with US-CERT's revised Incident Notification Guidelines, which require agencies to use an incident reporting methodology that classifies incidents by the method of attack, known as attack vector, and to specify the impact to the agency.[75]

During FY 2017, US-CERT initiated a process to validate its incident data with agencies to promote improved data quality. Table 18 details 35,277 incidents reported by agencies, and validated with US-CERT, across nine attack vector categories. This represents a 14% increase from FY 2016, when agencies reported 30,899 incidents. Email/Phishing continues to be a highly-targeted attack vector, with 7,328 incidents occurring in the past year. Moreover, nearly 31% 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.

Table 18: Agency-Reported Incidents by Attack Vector

Attack Vector	FY 2016			FY 2017		
	CFO	Non-CFO	Gov-wide	CFO	Non-CFO	Gov-wide
Attrition Employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	108	1	109	148	3	151
E-mail / Phishing An attack executed via an email message or attachment.	3,166	126	3,292	6,918	410	7,328
External / Removable Media An attack executed from removable media or a peripheral device.	132	6	138	71	1	72
Improper Usage Any incident resulting from the violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	3,920	210	4,130	7,575	281	7,856

[75] NIST, Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide (2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (listing common vectors that are the method of attack and provides expansive definitions of the attack vectors cited in this report).

Loss or Theft of Equipment The loss or theft of a computing device or media used by the organization.	5,313	377	5,690	4,102	293	4,395
Web An attack executed from a website or web-based application.	4,767	101	4,868	3,922	127	4,049
Physical Cause An attack or accident initiated in the physical realm.	--	--	--	7	0	7
Other The attack method does not fit into any other vector or the cause of attack is unidentified.	11,445	793	11,866	10,162	656	10,818
Multiple Attack Vectors An attack that uses two or more of the above vectors in combination.	789	17	806	579	22	601
Total	**29,640**	**1,259**	**30,899**	**33,484**	**1,793**	**35,277**

Major Incidents by Attack Vector

Of the 35,277 incidents reported in FY 2017, agencies reported five incidents that met the threshold for major incidents in accordance with the definition in OMB M-18-02. A summary these major incidents is provided below:

- **Department of Homeland Security**

  On May 11, 2017, the Acting CISO of DHS's Office of the Inspector General (OIG) reported to DHS officials that the sensitive personal information of 246,167 DHS employees had been discovered on the home computer server of a DHS employee. An additional 159,000 case files from the IG's investigative case management system were also found. On August 21, 2017, the Acting DHS Secretary notified two groups of affected employees: 1) those whose names appeared on a list as being employed by the department either in 2014 or in other years; and 2) individuals (i.e., subjects, witnesses, and complainants) associated with DHS OIG investigations from 2002 through 2014. DHS is coordinating the notice of additional impacted individuals and is offering an 18-month credit monitoring service subscription to all those affected. The impact of this breach is still being determined.

- **Department of the Treasury**

  On March 3, 2017, IRS identified a breach in which 100,210 taxpayers had their Adjusted Gross Income information exposed to unauthorized parties via

impersonation through its Data Retrieval Tool. The impact of this breach is Moderate.

- **Department of Transportation**

  On November 1, 2016, DOT identified and notified US-CERT, OMB, and Congress of an inadvertent disclosure on one of its public-facing websites. DOT determined that the breach was not a result of malicious intent or compromise. The impact of this breach is Low.

- **Federal Energy Regulatory Commission**

  A malicious actor attempted to compromise Commission employees' email accounts. As a result, email for six users was forwarded to an unauthorized source. Federal Energy Regulatory Commission is still determining the impact of this incident.

- **Office of the Comptroller of the Currency**

  Prior to retirement, a former OCC employee downloaded more than 10,000 encrypted files that included Controlled Unclassified Information (CUI) and PII to two removable thumb drives. The downloads occurred in November 2015 on a laptop part of the Network Infrastructure – General Support System, and were first detected on September 1, 2016. The impact of this breach is Moderate.

C. Agency Cybersecurity Performance Summaries

FY 2017 Annual Cybersecurity Risk Management Assessment

Advisory Council on Historic Preservation

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | While the Advisory Council on Historic Preservation (ACHP) does not deal with any classified assets, the loss (data loss) of HVAs would significantly impact agency operations. The risks to HVAs are primarily data loss and destruction. The biggest challenge for the agency is the lack of funding in addition to a lack of dedicated staff for cybersecurity operations. Over the last several years, ACHP has, both internally and externally, emphasized the importance of establishing a cybersecurity program and as a result, limited funding was made available at the end of FY 2017, which improved the agency's cybersecurity posture in several critical areas and the NIST Cybersecurity Framework capability gaps. This has resulted in a measurable reduction in risks.

Strategy | ACHP is aware of certain infrastructure risks due to resource and infrastructure limitations; however, the agency lacks a complete set of tools to manage threats and vulnerabilities. The known risks were presented to agency senior leadership and understood, which led the agency to request cybersecurity funds in its most recent budget request. FY 2017 funds for cybersecurity were ultimately constrained due to a budget shortfall. Most agency risks are accepted, with the goal of addressing those risks when funds become available. The primary approach is to prioritize fundamental capability gaps that have the highest impacts to reduce immediate risks.

Resources | As previously referenced, the ACHP has not had the resources to establish a full cybersecurity program. As a result, the agency has been constrained in establishing a full cybersecurity program. End of FY 2017 funds were utilized for high priority areas where there were significant capability gaps. Additional projects will be implemented in FY 2018 if funds can be allocated. Most of the agency funds are used for general operating costs.

ACHP has limited cybersecurity tools (e.g., anti-malware), and a lack of cybersecurity specialists on staff. Currently, the CIO who is also the CISO is the only staff with cybersecurity skills. Additional IT staff is limited to two staff members. The focus of the general IT staff is currently on operations, which inhibits their ability to perform a dedicated cybersecurity role. Funding shortfalls and continuing resolutions are the biggest problem in improving ACHP cybersecurity capabilities. While there were limited funds available within this FY to utilize for cybersecurity, the agency was able to implement significant improvements to its cybersecurity capabilities.

ACHP is currently participating in the DHS's CDM Program, which is assisting the agency in addressing some of the basic capability gaps as required in the NIST Cybersecurity Framework.

Leadership | ACHP senior leadership has been very responsive in the development and implementation of the agency's cybersecurity risk management strategy; however, the agency is constrained by the lack of overall funding to implement the plans.

The CIO/CISO communicates regularly with senior leadership (including the Executive Director) about cybersecurity risks. The Executive Director supports ACHP's plan to improve its cybersecurity posture through upcoming FYs, and has prioritized the program for funding access as feasible.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program ACHP was not performed for FY 2017, 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. ACHP will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

American Battle Monuments Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	3	2
Multiple Attack Vectors	0	1

CIO Risk Management Self-Assessment

Risks | The American Battle Monuments Commission (ABMC) has a unique mission prerogative of being open to the public. With this in mind, the agency must maintain operating conditions that support public and employee safety and security.

In the absence of a formal Risk Assessment process, the agency recognizes two types of cybersecurity risks:

1. Risks that might impact public or employee's safety and security; and
2. All other risks.

To mitigate this first risk, usually of an external nature, the agency is upgrading its network operations and infrastructure, by designing additional redundancy and security controls into its systems. For example the agency has invested in a world-wide cascade/alert system with the objective of reaching 100 percent of agency workforce in minutes of an incident. ABMC also distributed satellite phones to serve as alternate means of communication in the event host-country telecom infrastructures are disrupted.

The second category of risks covers operational security risks caused by inadvertent, deliberate action or inaction of people, system failures or failed internal process.

Strategy | The agency will be further refining and detailing its risk approach as it progresses on the path to Cybersecurity maturity.

Resources | The agency is developing additional capabilities to meet Cybersecurity prerogatives.

Leadership | Senior leadership plays an active operational role. Leadership recognizes the importance of Risk Management in general and has moved efforts on Circular A-123 to a strategic level; ABMC is formulating an implementation plan.

Inspector General Assessment

ABMC does not have an IG; therefore, it contracted an independent certified accounting firm to perform the assessment.

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

Our primary recommendations are for ABMC to update Plans of Action and Milestones and Cross-Agency Priority Goals based on the organizational change and to ensure its IT environment and infrastructure is part of their annual ERM process.

FY 2017 Annual Cybersecurity Risk Management Assessment

Armed Forces Retirement Home

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Armed Forces Retirement Home (AFRH) has identified that the agency's largest risk is continuous monitoring of the network, which is currently being conducted by a Department of the Interior data center. Although a few extraneous items have infiltrated the agency's network, investigations of the incident showed no impact on any of the identified HVAs or Mission Essential Functions of the agency.

Strategy | In order to address the weakness in continuous monitoring of the network, AFRH, in consultation with the Department of the Interior's Office of the Chief Information Officer (OCIO), was able to isolate the impacted system, terminate access by all users, and initiate a threat analysis in order to mitigate any potential harm to the network. The Department of Interior's OCIO implemented additional security measures and firewalls to protect AFRH's networks and HVAs. Following the implementation of these new measures, no other threats were discovered.

Resources | AFRH has not identified any gaps to mitigate vulnerabilities to its network or HVAs at this time. The agency has strongly supported the defense of cyber vulnerabilities by providing additional monetary resources.

Leadership | AFRH leadership integrates cybersecurity risk management efforts into the agency's overall Risk Management Strategy. Senior managers are briefed on the status of the agency's state of cybersecurity quarterly and are encouraged to make recommendations to improve the agency's posture and defense against cyber threats.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. Although documentation and validation have improved this year, AFRH continues to be deficient in its automation of risk management processes, validation of an enterprise architecture strategy, implementation of multi-factor authentication (such as PIV), and tracking of contingency plan testing. The AFRH will continue to improve upon its posture in the aforementioned areas in collaboration through its Federal Shared Services agreement with the Department of Interior's OCIO.

FY 2017 Annual Cybersecurity Risk Management Assessment

Barry Goldwater Scholarship and Excellence in Education Foundation

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 2017
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

FY 16: 0
FY 2017: 0

CIO Risk Management Self-Assessment

Risks | The Barry Goldwater Scholarship and Excellence in Education Foundation (BGSEEF) (the Foundation), in adapting to changing technology and security challenges, continually re-evaluates its security against cyber and physical intrusion. The Foundation is a low-risk security classified agency, maintaining no permanent electronic or paper records containing any private information. All information collected in fulfilling the agency's mission, personnel and obligations are through multi-point, monitored and protected intra-agency agreements with GSA and USDA OCFO. The Foundation's cybersecurity is monitored by DHS and by an independent contractor approved by the Federal Government.

Strategy | BGSEEF's financial transactions are conducted with the Department of the Treasury through an Intra-agency Agreement with USDA OCFO. The agency maintains no independently accessible accounts or monies. As a micro-agency that receives no annual appropriations, and by legislation is restricted in investment options, resources are guarded carefully. The minimal personnel and HR requirements at the Foundation are likewise handled by an Intra-agency Agreement with GSA. By size and mission, the Foundation is minimally at risk for attack of any sort, but is proactive in pursuing all avenues to mitigate any possible compromises.

Resources | The Foundation is constantly re-evaluating and revising the fundamental processes central to the agency's mission. An examination of internal reporting applications are being done following a recent restructuring of the Foundation's online nomination process.

Leadership | As a two-person micro agency, BGSEEF has a close relationship between Senior Leadership and staff. Discussions are held daily regarding issues the Foundation is facing. Agency-level decisions are made by the agency head.

Inspector General Assessment

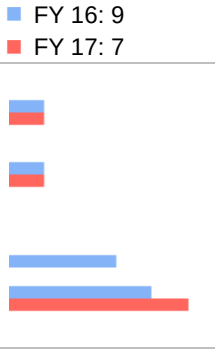
An independent evaluation of the status of the IT cybersecurity program for BGSEEF was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. The Foundation will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Board of Governors of the Federal Reserve

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	1
External/Removable Media	0	0
Improper Usage	1	1
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	3	0
Other	4	5
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | Primary cybersecurity risks to the Board of Governors of the Federal Reserve (Board) include 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. The Board's detection and prevention strategy includes, but is not limited to:

- Layered perimeter security that includes web content filtering, intrusion prevention, email filtering, Einstein 3A monitoring services, and Data Loss Protection;
- Next generation endpoint and network based security to decrease our exposure to zero-day attacks;
- Enforcement of two-factor PIV authentication for privileged users;
- Anti-DDoS protections;
- High availability configurations of high value systems;
- Conducting network monitoring for anomalies and suspicious activity; and
- 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.

In addition, the Board undergoes annual audits by the Board's OIG and has annual independent security assessments by third parties.

Strategy | If an IT risk is identified, the system and business mission owner, in consultation with Board information security staff, determines whether or not the risk can be resolved without adversely impacting business and mission operations. If the risk can be resolved, it is either resolved immediately, or documented as a Plan of Action and Milestones. Risks that cannot be resolved immediately are presented to management for acceptance consideration. If management does not accept the risk associated with a vulnerability exception, the system owner will create a Plan of Action and Milestones and track the remediation efforts until resolved.

Resources | The Board tracks and monitors gaps in meeting NIST defined requirements through Plan of Action and Milestones. The Board has identified three primary gaps that need to be resolved to address the highest priority risks: (1) enforcing two-factor PIV authentication for non-privileged users; (2) implementing Managed Trusted Internet Protocol Services (Einstein 1 and 2); and (3) implementing a formal insider threat program beyond the national security space. The Board has allocated the appropriate resources and initiated projects to address each of these gaps.

Leadership | Cybersecurity risk management is integrated directly into the Board's Strategic Plan (Plan), which is reviewed by senior leadership regularly. Plan of Action and Milestones are communicated to Authorizing Officials and affected stakeholders when identified, and are reviewed bi-annually.

The Board Information Security Officer annually briefs the governors on the Committee of Board Affairs (CBA) on the cybersecurity risk posture of the Board. The Board Chief Operating Officer and CIO are also briefed by the CISO on a frequent basis.

Inspector General Assessment

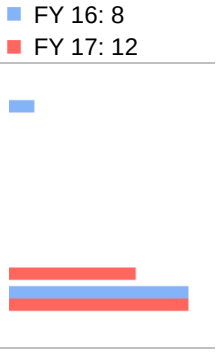
The OIG determined through independent review that the agency does not have an effective information security program. Overall, the OIG found that the Board continues to mature its information security program. The OIG also found that the Board's information security program includes policies and procedures that are generally consistent with the functional areas outlined in the NIST Cybersecurity Framework. However, the OIG identified opportunities to strengthen processes and controls in the areas of risk management, configuration management, identity and access management, Information Security Continuous Monitoring, and contingency planning to further mature the program and ensure that it is effective. The OIG audit report includes nine recommendations to strengthen controls in these areas.

FY 2017 Annual Cybersecurity Risk Management Assessment

Broadcasting Board of Governors

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	5
Other	7	7
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | BBG does not maintain any OMB-defined HVAs. Cybersecurity risks to Mission Essential Functions include the following:

- Enterprise Risk Management (ERM) strategy and program are not fully implemented, still leaving some risk management roles and responsibilities undefined;
- Rogue or misconfigured information systems may be connected to the network and are potentially vulnerable to exploitation;
- Staff understanding of enterprise or system-specific risk exposure is low due to scarce resources to perform risk assessments;
- Comprehensive information security policies and procedures are not finalized;
- Incomplete deployment of multifactor authentication;
- Inconsistent system patching;
- Limited role-based training limits system administrators' ability to protect;
- Limitations in scanning encrypted network traffic;
- Inconsistent management of privacy data;
- Security events might go undetected due to lack of comprehensive security event monitoring;
- Malicious activity may go undetected due to an immature continuous monitoring program;
- Incident response might be delayed due to lack of surge resources.

Strategy | The BBG's strategic plan has long embraced the following strategies:

- Migrate most applications and content distribution to the cloud;
- Consolidate applications and co-locating data centers within the agency; and
- Virtualized servers.

BBG has also significantly reduced and mitigated network infrastructure risk by implementing a plan to enhance network resilience and by deploying several internally-built defenses and monitoring tools. These will be supplemented with tools and capabilities of DHS's CDM, Privileged Management, and Einstein 3A programs. To fill remaining gaps, the BBG is investing in several commercial network, email, and host-based defenses and tools.

Given scarce resources, BBG has increased risks for its digital audio and video editing tools as they are extremely network bandwidth-intensive and technically complex, and cannot be transferred to cloud service solutions. However, BBG has made every effort to mitigate risk through the on-premises redundancy and resiliency efforts.

Resources | Due to budget limitations, BBG's ERM program and associated supporting programs and activities require further development. Additional gaps include:

- Insufficient staff to complete periodic risk assessments for all BBG systems;
- Inconsistencies with agency IT security policy and procedures. Work has begun to adapt the comprehensive cybersecurity policy framework from DHS to BBG's use;
- Nascent role-based training for system administrators;
- Lack of tools for monitoring encrypted Internet traffic for malicious behavior. Additional funding is needed for SSL decryption technology;
- Inconsistent management of privacy data. Additional funding is needed for Data Loss Prevention (DLP) tools;
- Nascent continuous monitoring program. The agency is participating in the DHS CDM program, but additional staffing and tools will be needed to complete the program; and
- Inconsistent enterprise and system-specific contingency policies, plans, and procedures.

Leadership | The Chief Executive Officer (CEO) is taking action to implement an ERM program and is monitoring BBG's progress on the FISMA gaps. BBG has adopted the NIST Cybersecurity Framework and integrated the core principles at the department-level within the scope of the technology programs managed by the OCIO.

BBG drafted an update to the CIO's delegation and has drafted a directive to the CIO to develop both an information security risk management strategy and a draft CIO Council Charter for agency review.

Inspector General Assessment

Acting on behalf of the OIG, an Independent Public Accounting firm conducted an audit to determine the effectiveness of information security program and practices in FY 2017. The Independent Public Accounting firm concluded that BBG has not realized an effective organization-wide information security program for three fundamental reasons. OIG is recommending that BBG's CEO and Director: (1) update and clarify CIO

delegation documents related to information security program governance; (2) direct all offices, as well as all Federal and grantee broadcasting networks, to report identified risks to the Risk Management Division and codify this requirement; and (3) develop and implement an organization-wide information security risk management strategy that aligns risk management decisions with business functions and objectives within a mandated timeframe.

FY 2017 Annual Cybersecurity Risk Management Assessment
Chemical Safety Board

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

The Chemical Safety Board (CSB) did not provide an assessment regarding their cybersecurity-related risks, strategy, leadership, and resources.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. CSB has demonstrated they have defined policy, procedures and strategies for all five of the information security function areas.

Additional testing was conducted for the Patch Management processes to determine whether the agency implemented the noted Patch Management policies, procedures and strategies to achieve a higher maturity level. This process was found to be effective as implemented and rated at Level 5 - Optimized.

Several areas within the CSB's information security program were identified at Level 1 – Ad Hoc. Based on our analysis, improvements are needed in the following areas:

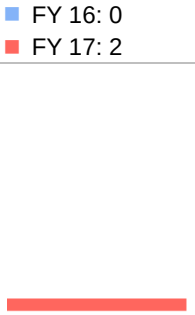
- Identity and Access Management: CSB does not include fully defined processes for PIV card technology for physical and logical access.
- Incident Response: CSB has not identified nor fully defined its incident response processes or technologies to respond to cybersecurity events.

FY 2017 Annual Cybersecurity Risk Management Assessment

Commission of Fine Arts

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	2
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Commission on Fine Arts' (CFA) vulnerabilities include: implementation of policies and development of procedures, account management, configuration baseline, password complexity, user ability to install software, patching, web encryption, and cross-site scripting. The overall security posture was deemed satisfactory by the most recent security assessment, and the vulnerabilities discovered were more likely to be problematic for internal, rather than external, sources. Nevertheless, the CFA acknowledges the need to address them to the best of its capacity. A lack of staff resources and expertise also constitutes a cybersecurity risk to the agency.

Strategy | Implementing EINSTEIN 3A initiatives has helped manage potential threats that originate from external sources. User education has increased, particularly for risks inherent in email usage. In addition, there is a redoubled effort to ensure that all vendor updates and patches are automated. While the agency is making progress, due to budget and resource restraints, CFA is forced to accept the risks connected with vulnerabilities related to account management, configuration baseline, and the formulation of policies and procedures.

Resources | The most significant gap the agency faces in its cybersecurity posture is knowledgeable and dedicated staff or access to personnel with the capacity to fully address the CFA's cybersecurity infrastructure. CFA strives to leverage its existing resources as much as possible, but additional staff and financial resources would help increase the agency's overall security posture.

Leadership | CFA's senior leadership is apprised of risks whenever necessary, with regular briefings on the planning and implementation of all cybersecurity initiatives. Senior leadership serves as signatories to all necessary reports, agreements, and data calls. Limitations in funding and staffing are a challenge for senior leadership, forcing the need to balance programmatic functions with support functions.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for CFA was not performed for FY 2017, 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. CFA will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Commission on Civil Rights

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	2	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The United States Commission on Civil Rights' (USCCR) risk assessment of its data and information systems includes risks to the agency's HVAs, Mission Essential Functions, and intra-agency security reviews.

USCCR evaluates three elements from its master risk register to include risk probability, impact, and exposure. The Commission assesses and analyzes the likelihood of risk, inventoried IT systems, and data to create an individualized list of the risk's impact to each system. This allows the agency to identify vulnerabilities, and develop a risk mitigation strategy for operations staff and contractors to appropriately prioritize and manage risks.

Strategy | USCCR planning activities are carried out by the agency's IT security and operations teams, which enable staff to prioritize the risks and develop mitigation strategies. USCCR management aims to have all risks mitigated on time and on budget; however, certain risks are unable to be fully resolved due to budget, personnel, resources, and processes. The agency prioritizes what risks it mitigates, transfers, or accepts according to its resources. The agency is forced to accept some risks based on the likelihood of occurrence, impact of exploitation, and cost of implementation. The decisions on the agency's risk strategies are documented, tracked, and managed according to the agency's risk management policy.

Resources | USCCR's risk assessment revealed gaps across all of the NIST Cybersecurity Framework functions and domains. The agency plans to address the gaps to improve the security posture of the agency.

Leadership | USCCR senior leaders stay apprised of risk within the enterprise by receiving monthly vulnerability reports and briefings on vulnerability mitigation plans. USCCR senior management develops the budget and assigns responsibility for mitigating identified risks. Further, USCCR leadership is required to sign off on risks the agency decides to "accept".

USCCR senior management is in the process of acquiring the necessary cybersecurity skill set through contracting to help protect the agency's assets and improve the agency's security posture.

Inspector General Assessment

USSCR contracted with an independent auditor to conduct the FY 2017 independent evaluation of its information security program and practices as a performance audit under Generally Accepted Government Auditing Standards. The auditors for USCCR 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 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 Plans of Action and Milestones already identified and to ensure that the policies and procedures outlined in the Plans of Action and Milestones are successfully addressed in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Commodity Futures Trading Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	0	1
External/Removable Media	0	0
Improper Usage	1	1
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	1	2
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | Facing risks similar to those of other agencies, Commodity Futures Trading Commission (CFTC) has built an Enterprise Information Security Program that engages in policy and compliance activities to protect Commission assets and mission functions. While policies and handbooks have been established, they have not been fully implemented.

CFTC has, through various assessment processes, identified several IT security risks. The first is weaknesses related to internal controls, specifically access controls, continuous monitoring controls, and boundary protection management practices designed to protect mission essential functions. CFTC also needs to improve on the timely remediation of system security vulnerabilities on network devices, server platforms, and web applications. Going forward, efforts will focus on establishing effective processes to ensure timely corrective actions are implemented on outstanding system security risks.

Protecting HVAs and Mission Essential Functions also requires capabilities and resources that are not yet in place, including an Insider Threat Program, automated tools, and predictive and preventative technologies.

Strategy | CFTC's risk management strategy is guided by various NIST publications and provides due-care by addressing specific risk factors. CFTC has taken the following preemptive steps to reduce risk to the enterprise:

CFTC has a formal change and configuration management process to manage the risk of IT changes being introduced in the environment.

CFTC's Enterprise Information Security Program conducts a Security Impact Analysis to assess each change to the enterprise for IT risks or control weaknesses.

CFTC is creating an enterprise cybersecurity risk register to document, monitor, and manage system security risks and implement risk mitigation controls. It will allow CFTC to prioritize and manage risks using a calculated risk value.

The organization's ability to achieve its goals depends on its ability to capture, process, manage, analyze, prioritize, and share information with customers and counterparts in the Federal IT community.

Resources | In 2016, CFTC began adopting the NIST Cybersecurity Framework. The organization actively assesses the current and desired maturity for each cybersecurity service, including planned projects, acquisition of tools and technology, personnel needs, and the corresponding budget requirements. CFTC has also made progress aligning with the NIST National Initiative for Cybersecurity Education (NICE) to identify resource, functions, training, and workforce development needs.

Key gaps that have been identified in the organization's information security program include:

- Fulfillment of the DHS CDM program;
- Timely remediation of Plan of Actions and Milestones on major systems;
- Role-based security training;
- Automated patch management;
- Privilege account and identity, credentialing, and access management;
- Full compliance with PIV usage targets;
- Development of an insider threat program;
- Security policy enforcement;
- Governance, risk and compliance capability, including people, processes, and technology;
- Expand the Enterprise Data Loss Prevention capability; and
- Establish and formalize senior management committees on ERM.

Efforts are currently underway to address a subset of these gaps, and resource planning is aligned to ensure all gaps are addressed.

Leadership | CFTC's CIO and CISO meet with the Chairman, the Senior Accountability Official, and other members of agency's senior leadership on a monthly basis to brief them on topics related to cybersecurity, include existing risks, budget adjustments, and progress aligning the organization's needs to various NIST Frameworks, including the NIST Cybersecurity Framework. Meetings are more frequent in response to specific threats or events. The Chairman also signs a statement of assurance on CFTC's cybersecurity posture, which is based on the results of various assessments and reviews.

Inspector General Assessment

CFTC's information security program generally meets standards prescribed by the FISMA. Specifically, CFTC's information security program addresses each of the FISMA domain requirements and is deemed "Effective" when measured against the FISMA security framework. While CFTC has improved its information security posture, we re-highlight remaining security concerns made in FY 2016 related to maturing Insider Threat and ERM Programs. For FY 2017, CFTC's information security

program can improve its incident response procedures and integrate security investment planning into an overall Enterprise Architecture program.

Outstanding Recommendations:

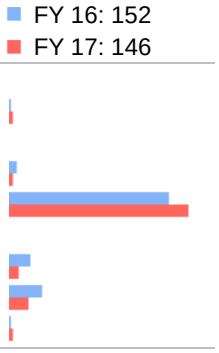
1. Mature an Insider Threat Program;
2. Mature overall ERM program;
3. Improve Incident Response procedures and resources; and
4. Integrate security investment planning in an overall Enterprise Architecture program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Consumer Financial Protection Bureau

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	2
External/Removable Media	0	0
Improper Usage	5	3
Loss or Theft of Equipment	108	120
Physical Cause	NA	0
Web	15	6
Other	22	13
Multiple Attack Vectors	1	2



CIO Risk Management Self-Assessment

Risks | The Consumer Financial Protection Bureau (Bureau) uses internal security assessments, continuous monitoring activities, and audits to identify cybersecurity risks and opportunities to gain efficiencies. Results inform decisions regarding:

- Achieving and maintaining visibility into data and assets in a distributed IT environment that embrace the shared service models of FedRAMP and Federal service providers;
- Addressing data protection needs while interfacing with the public;
- Achieving near real-time situational awareness to cyber threats and vulnerabilities; and
- Safeguarding sensitive information from misuse or alteration.

The Bureau is focusing on a risk-based approach that employs the NIST RMF and Cybersecurity Framework to identify and manage risk to HVAs and mission essential functions.

Strategy | The Bureau's approach balances mitigating risk with the implementation of cost-effective and feasible measures, accepting risk based on business context, or transferring risk to a third party where appropriate.

The Bureau pursues compensating mitigations to reduce the overall risk to an acceptable level in accordance with the FISMA.

The agency uses shared services and adopts a cloud-first strategy to meet its technology needs and make deliberate decisions to transfer risk to its third party service providers. The Bureau monitors the risk associated with these service providers by leveraging trust relationships, reviewing partner agency and FedRAMP system authorizations, and conducting risk assessments of third-party service providers.

Resources | While CFPB's IT program continues to evolve independently from Treasury, many processes are still manual with challenges ranging across scalability, a remote workforce, and drive for enhanced efficiency. Investments and innovations in technology, data, and process are regularly introduced and reviewed against risk, feasibility, and other factors to efficiently and effectively use limited resources and overcome challenges.

The Bureau established an ERM program and is refining its approach to identifying and assessing mission essential functions and HVAs using a thorough business impact analysis. As a result, risk-based decision making will be better informed by business priorities. The Enterprise Risk Committee is the central ERM governance body for cybersecurity risk management across the RMF functions.

Leadership | Senior leadership plays a critical role in the development and ongoing implementation of the Bureau's cybersecurity risk management strategy. In accordance with FISMA and Circular A-123, the Director is informed of critical risk management decisions through the ERM program, and consults with senior leadership regarding mitigation strategies, status, and allocation of resources.

The CIO serves as the authorizing official for cybersecurity risks and establishes an acceptable level of risk, deploys mitigation resources, and decides to accept risks that cannot be mitigated or transferred. The CIO considers cybersecurity risk in the context of Bureau operations and business functions when making authorization decisions.

Inspector General Assessment

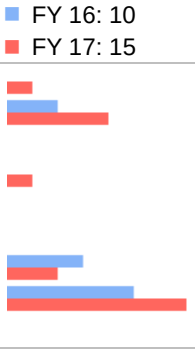
The OIG determined through independent review that the agency does not have an effective information security program, but continues to take steps to mature it. We found that the CFPB's information security program includes policies and procedures that are generally consistent with the functional areas outlined in the NIST Cybersecurity Framework; however, we identified opportunities to strengthen processes and controls in the areas of risk management, configuration management, identity and access management, security training, incident response, and contingency planning to further mature the program and ensure that it is effective. Our audit report includes seven recommendations to strengthen controls in these areas.

FY 2017 Annual Cybersecurity Risk Management Assessment

Consumer Product Safety Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	2	4
External/Removable Media	0	0
Improper Usage	0	1
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	3	2
Other	5	7
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Consumer Product Safety Commission (CPSC) has made considerable progress in addressing gaps in its information security policies, procedures, and practices that have led to improved ratings on two of the NIST Cybersecurity Framework function areas as well as a 63% reduction in OIG FISMA findings from the previous year. The agency suffered no major information security incidents in FY 2017 and reported a total of seven non-major incidents to US-CERT.

Areas of significant progress for the agency's information security program include the development and testing of contingency and configuration management plans for the agency's major systems and its GSS, enforcement of two-factor PIV authentication for all non-privileged accounts, coordination with the CFO and other program executives in the development of an agency-wide risk management strategy, implementation of hardware and software asset management tool, implementation of advanced persistent threat protection capabilities, and agency-wide phishing/malware detection testing. The agency also worked with DHS to implement monitoring and diagnostics and to prepare the agency for inclusion in the Continuous Diagnostic and Monitoring program.

Strategy | CPSC tracks all identified vulnerabilities (i.e., exploitable weaknesses) through an enterprise security assessment and management system. Vulnerabilities are assessed and prioritized based on risk and impact. Implementation is tracked and reported on a regular basis.

In FY 2018 CPSC intends to enforce two-factor PIV access for privileged accounts, migrate to a new anti-virus solution, identify automated tools to streamline patch management, and increase the integration of IT security and enterprise risk management frameworks.

Resources | The agency is prioritizing activities within the information management programs to provide increased focus on accomplishment of the FY 2018 information security -related priorities. The agency has requested additional funding for FY19 to support increasing requirements for the protection of privacy information. The agency is also re-evaluating the potential for automated system testing capabilities to help streamline these processes.

Leadership | Agency leadership is aware and supportive of information security improvement efforts. Both the CIO and CISO are integrated into the agency executive risk management function.

Inspector General Assessment

Based on the maturity model scoring methodology set out in the government-wide OIG metric requirements, the CPSC reached level 4, "Managed and Measurable", in both "Function 3, Detect-Information Security Continuous Monitoring ", and in "Function 4, Respond-Incident Response." However, it was at level 1, Ad Hoc, in the three remaining functions. As a result, OIG determined the CPSC's information security program to be "Not Effective."

The CPSC has continued to make improvements in its IT security program and progress in implementing the recommendations resulting from previous FISMA evaluations. OIG attributes many of the issues identified in this year's assessment to a lack of resources necessary to support the implementation of planned information security activities.

FY 2017 Annual Cybersecurity Risk Management Assessment

Corporation for National and Community Service

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	4	2
External/Removable Media	0	0
Improper Usage	1	0
Loss or Theft of Equipment	14	4
Physical Cause	NA	0
Web	1	1
Other	5	6
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Corporation for National and Community Service (CNCS) considers its cybersecurity risk level to be “At-Risk.” The agency has policies, procedures, processes, and tools in place that meet the baseline requirements of the NIST Cybersecurity Framework functions, but there is room for significant improvement and additional capabilities.

Strategy | CNCS's approach to managing identified risks are based on general vulnerabilities revealed during system scans or reports from US-CERT. The majority of the identified risks are mitigated based upon an established timeframe. In some instances, CNCS is forced to accept risks due to business requirements or budget constraints. All risk acceptances are reviewed by all system stakeholders to ensure all parties are aware of the risk being added to a specific system. At this time, CNCS is unaware of any known threats against the agency.

Resources | CNCS perceives funding as a gap in achieving implementation of multi-factor authentication (example; PIV) and contractor authentication.

The agency also currently has a shortage of knowledgeable personnel and established methods and tools for monitoring and analyzing information from its Security Information and Event Management (SIEM) tool.

Leadership | The CISO is responsible for cybersecurity risk management through a process of Plans of Action and Milestones and Information Security Continuous Monitoring to manage and identify potential vulnerabilities. Information system cybersecurity risks are conveyed as needed to the CIO and the IT Steering Committee to allocate resources. When an identified risk impacts the entire enterprise, the CISO will use the ERM program comprised of a Risk Assessment Committee and the Risk Management Council, both of which meet quarterly.

Inspector General Assessment

CNCS has devoted significant resources to improving cybersecurity over the past few years, with meaningful progress. Although its information security program is not yet sufficiently mature, it can reach effectiveness with continued effort and investment.

Achieving effectiveness will require attention to weaknesses that pose significant risks to information security. The OIG, through independent review in 2017, found inadequacies in risk management, configuration management, identity and access management, information security continuous monitoring, and contingency planning. Enforcement of information security is inconsistent across the enterprise, with field components remaining especially vulnerable. These continuing vulnerabilities leave CNCS operations and assets at risk of unauthorized access, misuse and disruption. CNCS’s report offers 34 recommendations to address the identified weaknesses and assist CNCS in strengthening its information security program. Eight of the recommendations relate to prior findings that have not been completely addressed by CNCS.

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	High Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | CIGIE relies on the use of cloud-based service providers to perform most of its critical functions. CIGIE maintains a vigilant approach with these providers to ensure they are meeting FedRAMP requirements and to resolve any cyber-related incidents.

Although exposure to the public internet creates a constant risk, CIGIE does not believe its cloud providers represent an imminent risk to the operations of the agency.

CIGIE owns and maintains a system that provides internet access to agency employees called the General Support Services (GSS). This system allows the two agency locations to exchange information, and facilitates data storage. CIGIE has recently taken steps to improve its cybersecurity posture to ensure that the system meets Federal mandates and NIST standards.

CIGIE has identified two high priority risks. The first is the in-progress enhancement of the CIGIE GSS. To mitigate this risk, CIGIE has upgraded security appliances and has implemented best practices for cybersecurity management and protection controls including advanced monitoring tools.

The second major risk is data protection. CIGIE is currently reviewing all existing data sources and repositories for compliance, integrity, confidentiality and availability.

CIGIE also identified three medium-priority risks: cybersecurity awareness, workstation protection, and mobile device protection. To address cybersecurity awareness, the agency provides users with the information needed to manage cybersecurity challenges and risks. Users are frequently reminded about best practices and provided with specific actions to prevent malware infection. To further workstation protection, CIGIE is carrying out a project to replace all agency laptops using a new and improved OS image that follows NIST standards for configuration. To better protect and manage mobile devices, CIGIE will implement Microsoft Intune across all mobile devices in the agency.

Strategy | Hosting websites creates a constant exposure to the public internet and therefore presents a risk. In response, CIGIE has transferred the risk of hosting its website presence and operations to a cloud service provider. CIGIE also leverages the DHS NCATS team to perform periodic security assessments of agency websites, with remediation efforts assigned to a specialized contractor. In addition, CIGIE performs vulnerability scans of these resources, recording and managing any findings as part of the Continuous Monitoring and Diagnostic process. CIGIE transferred productivity functions, including email to FedRAMP-compliant cloud service providers. These providers deliver cybersecurity services that ensure the normal operation of agency activities.

CIGIE continues the process of mitigating potential risks to the system it owns and maintains by enhancing and modernizing perimeter protections. As part of these efforts CIGIE recently deployed the following security controls: Application Control, Web Filtering, Perimeter Malware Protection, Geolocation Protection, Intrusion Prevention, Repudiation Defense, Botnet Protection and other security technologies that will increase the protection of agency assets. In addition, CIGIE is in the process of ensuring that all the system's components meet NIST and FISMA requirements and is aggressively pursuing compliance. CIGIE is discussing the implementation of CDM capabilities with DHS.

Resources | As indicated in the Risks section, CIGIE has focused its immediate efforts in addressing two high priority risks: enhancements to the CIGIE GSS and data protection. Although critical cybersecurity controls have been deployed, there are other functional enhancements planned for the GSS regarding migration to the cloud. Migration of the GSS to the cloud will address inefficiencies and improve service delivery capabilities to support the agency's mission. To reach this goal, the agency is reviewing the existing Office 365 contract, and will update it to include cloud migration and work with a contractor team to migrate the LDAP and folder repositories to the cloud using Microsoft Federation Services and SharePoint online. The agency's current plan is to use SharePoint online to support all file repository operations inheriting the FedRAMP capabilities that this infrastructure provides.

With regard to data protection, over the last few months the agency has implemented a short-term plan to ensure that its data is cataloged, backed up, archived, and protected. Going forward the agency's goal is to move its data up to the cloud using Office 365 and use the existing technical and security controls of this platform to address data protection.

Leadership | Agency senior management is supportive and attentive to the management of cybersecurity risks and strategy. To this end, CIGIE is updating its Risk Management Strategy, which includes the following key areas:

- Planning and budgeting
- Governance
- Leadership and workforce
- IT investment management
- Information management and access
- Privacy and information security

- Electronic signatures
- Records management
- Leveraging the evolving internet

Inspector General Assessment

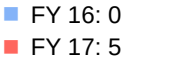
An independent evaluation of the status of the IT cybersecurity program for Council of the Inspectors General on Integrity and Efficiency was not performed, for FY 2017. Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. Council of the Inspectors General on Integrity and Efficiency will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Court Services and Offender Supervision Agency

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	1
Other	0	4
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | Based on a Court Services and Offender Supervision Agency (CSOSA)-wide review the following cybersecurity areas were considered to be “High Risk” or “At Risk”:

- Development and implementation of a formal risk management strategy and risk assessment procedures;
- Role-based security awareness training program; Incident response plan, procedures, processes, and capability;
- Enterprise information security and audit/log management architecture; and
- Full implementation of the Information Security Continuous Monitoring program.

Strategy | CSOSA’s Information Security Office will be developing a Risk Management Strategy that addresses how CSOSA will assess, respond to, and monitor risk. Criteria for the Information Security Continuous Monitoring program will be defined by the agency’s Risk Management Strategy. Under that strategy, CSOSA’s Executive Leadership will ensure that the agency’s Information Security Office administers an effective Information Security Continuous Monitoring program and will maintain high-level communications and relationships among organizational entities.

Currently, the agency mitigates risk through participation in the CDM program and through implementation of EINSTEIN 3A DNS Sinkholing capability, in addition to vulnerability and compliance management, endpoint anti-malware, threat/incident response and forensics, penetration testing, and threat detection capabilities, CSOSA has also implemented a network admission control capability to identify and quarantine unauthorized devices or non-compliant endpoints.

Resources | CSOSA used the NIST Cybersecurity Framework functions self-assessment results to prioritize gaps and develop action plans to help improve the agency’s ability to manage and reduce risks.

Leadership | The CSOSA CISO ensures visibility of cybersecurity risks and gaps in FISMA metrics. The CISO also briefs the Director on a monthly basis regarding cybersecurity risks within the enterprise. Moving forward, the CISO will provide more detailed monthly briefings to both the Directors of CSOSA on key information security issues and performance metrics.

The agency’s forthcoming Risk Management Strategy will also incorporate agency protocols for routine engagement and participation of CSOSA’s Executive Leadership teams.

Inspector General Assessment

An independent assessment group found that the agency does not have effective information security program. This group found that CSOSA and PSA have made progress in addressing previously identified information security deficiencies; however, a number of open deficiencies from previous years’ audits are still being addressed. Additionally, new deficiencies were also found in FY 2017. Based on the assessment of CSOSA’s information security program, its maturity level is determined to be between Level 1: Ad-hoc, and Level 2: Defined.

FY 2017 Annual Cybersecurity Risk Management Assessment

Defense Nuclear Facilities Safety Board

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	1
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	1
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | In late FY 2016, the Defense Nuclear Facilities Safety Board (DNFSB) senior leadership decided to invest additional resources in the IT enterprise. The CIO developed a multi-year plan to operationalize critical processes and execute a significant reduction in backlog initiatives. In preparation for FY 2018, DNFSB senior leadership is reviewing all avenues to reduce the agency's operational costs. DNFSB is reviewing, and possibly targeting, offsets for the IT environment. A budget reduction in IT would significantly impact the ability of the CIO to meet the agency's dynamic demands due to legislative, operational, and cybersecurity requirements.

Due to the prevalence of emails from outside resources, phishing attempts could increase if user behaviors are not aligned with safe cybersecurity practices.

Strategy | DNFSB self-assessments through the annual FISMA review process, in addition to the OIG reviews, help the agency to identify and manage risks. The CIO ensures identified risks are evaluated and the risk mitigation options are discussed at Configuration Control Board meetings and other appropriate venues. The IT staff developed a Plan of Action and Milestones that is continuously monitored and briefed to the CIO on a monthly basis. The CIO presents risks to the agency's General Manager (also the Senior Accountable Official) and Deputy General Manager on an as-needed basis.

DNFSB balances the usage of programs and guidance provided by larger agencies such as DHS with the time and effort participating in such programs takes. DHS program implementation delays may result in greater risk to DNFSB.

Resources | The agency's CIO and IT staff have reviewed the agency's shortfalls and they have divided these challenges into three major categories: automated tools, policy, and DHS capabilities, with plans to address each area.

Leadership | The agency's General Manager, Deputy General Manager, and the Division of Operational Services Director, are key stakeholders for DNFSB's cybersecurity risk management strategy. The agency head has situational awareness of the cybersecurity environment through the SAO, Deputy GM, and Director of DOS.

The CIO provides cybersecurity updates through a variety of means including, but not limited to, the use of weekly staff meetings, weekly activity reports and daily interaction to the SAO and Deputy GM. In short, the majority of IT budgetary decisions are made at the senior agency level.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. DNFSB has continued to make improvements in its information security program and has completed implementing recommendations from previous FISMA evaluations; however, the independent evaluation identified the following information security program weaknesses: 1) Information security program documentation is not up-to-date; and 2) Information system contingency planning needs improvement. In addition, DNFSB has not developed qualitative and quantitative performance measures for several information security program areas. DNFSB is in CDM Group 2F and was not a part of the voluntary CDM Phase 1. DNFSB is actively participating in CDM task order 2F as a part of Wave 3.

FY 2017 Annual Cybersecurity Risk Management Assessment

Denali Commission

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | Vulnerability scan results during this FY found no major threats to agency security.

Strategy | Denali Commission uses the United States Treasury Shared Services systems. The agency 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 within the Treasury, to provide much of their IT security.

Resources | Denali.gov utilizes an older version of its content management system. The Commission is in the process of procuring services to update the website as well as a newer content management system.

Leadership | The management team is briefed following the completion of vulnerability scans and following the completion of the annual FISMA assessment.

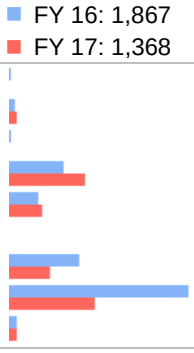
Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. In past years, due to the small size of the agency, much of the NIST Cybersecurity Framework was not applicable to Denali because the information was not kept within their network. Denali's information security program does not have fully documented and sufficient policies and procedures to identify, protect, detect, respond, and recover components of the NIST Cybersecurity Framework. Although the information security program could use improvement, the agency is still at a relatively low risk of encountering cyber-attacks due to the amount and type of information stored within its network.

FY 2017 Annual Cybersecurity Risk Management Assessment
Department of Agriculture

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	4	0
E-mail	27	40
External/Removable Media	1	0
Improper Usage	293	413
Loss or Theft of Equipment	155	182
Physical Cause	NA	0
Web	381	226
Other	965	464
Multiple Attack Vectors	41	43



CIO Risk Management Self-Assessment

Risks | USDA is a highly decentralized, federated, Department, with each bureau and subcomponent taking responsibility for IT and security resources. Many of the risks identified by the OIG result from USDA's federated system and the choices made at the programmatic level to direct spending to program-related activities or cybersecurity efforts. USDA has identified the following high-priority gaps and risks:

- Aging infrastructure combined with adoption of emerging technologies to support business; and requirements outpacing our oversight capabilities; and
- Limited inspection of network traffic; only 30 percent of inbound network passes through web-content filtering; and 0 percent of outbound network traffic is checked to detect unauthorized and encrypted exfiltration of USDA information and data; and
- Insufficient workforce to address all cybersecurity program requirements efficiently and effectively; and
- Outdated infrastructure supporting HVAs and mission essential functions. These systems face increased demands as more users expect mobile and remote access capabilities; and
- Additional risks include: Increased risk from cloud migration, securing the Internet of Things, evolving compliance mandates, and threats from social engineering attacks.

Strategy | USDA tracks IT risks across its bureaus through compliance programs and integrated scorecards under its RMF, which aligns with NIST's Cybersecurity Framework. Remediation of high-priority risks are evaluated and briefed to the CIO. Additional information is shared with OCIO Executive Leadership and the IT Risk Board. The scorecards are then reviewed with bureau CIOs to track critical risk areas.

The CIO must fully authorize all cyber risk-based decisions before releasing investment funds. USDA leverages department-level investments and systems to minimize, consolidate, remediate and manage risks to IT infrastructure and operations.

USDA enforces central management for mobile devices to ensure its burgeoning inventory is secured. In addition, cloud security requirements are being woven into the network modernization efforts, to allow program needs sufficient flexibility without redundant security costs.

Resources | USDA's OCIO funding for enterprise cybersecurity oversight and operations spending is less than one percent of total IT spending. While IT funding at the Department has increased, cybersecurity spending has declined from 2011-2016. This has hindered the Department's ability to recruit and maintain a strong cyber workforce and ensure it is staying on top of the latest threats.

USDA has also identified the following mitigating strategies to address the gaps that the IG identified:

- Proactively drive lifecycle management for enterprise IT infrastructure, tools, and licenses to maximize hardware and software duration and flexibility; and
- USDA is deploying DHS CDM Program solutions, although it is contingent upon receiving the requested funding increases for Operations and Maintenance of the CDM assets; and
- Leverage existing IT security staff through ongoing advisory council/process improvement teams to leverage best practices across USDA; and
- Migrate government off-the-shelf and commercial off-the-shelf tools to open source in order to reduce procurement, training, and operational costs.

These strategies reduce the impact of ongoing budget cuts; however, continual resource reductions are unsustainable and increase risks to USDA's IT and business processes.

Leadership | IT security is an executive priority beginning with the Secretary. IT risk is an integral part of the evolving ERM practice (per OMB Circular A-123). All business owners are required to assess the sensitivity and mission criticality of their data and processes, and integrate it with the USDA RMF.

USDA's Cybersecurity Strategic Plan aligns with the OCIO IT Strategic Plan and USDA Strategic Plan, balancing mission goals and objectives with cybersecurity protections. USDA manages operational, technical, and managerial risks throughout the lifecycle of all IT systems by engaging OCIO and agency executive leadership at all levels in this process. Governance includes the RMF, after-action reports, and Capital Planning and Investment Control processes and Executive Leadership forums, including the USDA CIO Council, IT Risk Management Board, and Information Security Steering Committee.

The CIO has a direct line to the Secretary, bureau administrators, and executive boards to address emergent cybersecurity risks and postures as well as monthly status briefs. This includes biweekly briefs/meetings with USDA's CIO Council and security staff to address specific cybersecurity hygiene factors.

Additionally, within USDA, all cybersecurity controls and processes are documented, implemented, and assessed at least annually to ensure protections against fraud, waste, and abuse. Finally, the Executive Review Board for IT Investments ensures

funding is expended to comply with FISMA and the RMF. OCIO executive leadership reviews IT portfolio investments annually for compliance with regulations before any IT expenditure over the minimum threshold is authorized.

Inspector General Assessment

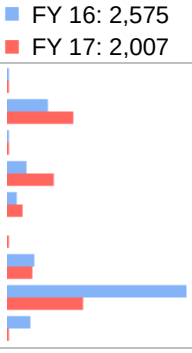
USDA OCIO continues to take positive steps in improving the USDA's security posture. For instance, implementation of the CDM program should allow the agency to increase network sensor capacity, automate sensor collections, and prioritize risk alerts. USDA's OIG found that the Department's maturity level for the five function areas to be at Level 2, "Defined", which under OMB criteria is considered ineffective. USDA needs to implement its controls and determine if they are operating as intended and are producing the desired outcome. Due to the new IG rating methodology, any historical comparison to past USDA ratings is not appropriate.

For FISMA audits from 2009 through 2016, OIG made 67 recommendations for improving the overall security of USDA's systems. 40 of the 67 recommendations have been closed, one open recommendation has not surpassed its implementation date, and the remaining 26 open recommendations are overdue. Testing this year identified that security weaknesses still exist for five closed recommendations. The remaining outstanding recommendations address weaknesses related to these five recommendations; therefore, it was determined that no new recommendations were warranted.

FY 2017 Annual Cybersecurity Risk Management Assessment
Department of Commerce

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	5	15
E-mail	346	567
External/Removable Media	5	1
Improper Usage	175	407
Loss or Theft of Equipment	87	131
Physical Cause	NA	2
Web	232	210
Other	1,531	653
Multiple Attack Vectors	194	21



CIO Risk Management Self-Assessment

Risks | Historically, the Department of Commerce's (DOC's) federated nature has resulted in the segmented identification and management of risks within each of its bureaus. However, through the implementation of FITARA, and by partnering with its bureaus, DOC has taken steps to incorporate cybersecurity risks into an ERM process. As a result, a number of enterprise cybersecurity risks have been identified and are being managed at either the enterprise- or bureau-level. Key cybersecurity risks include:

- Lack of real time continuous monitoring capabilities to facilitate standardized risk-based information security management;
- Deficiencies in identifying vulnerabilities, remediating security controls expeditiously, and managing access controls effectively;
- Inadequate authentication tools and implementation;
- Inability to attract, hire, and maintain staff needed to maintain security processes on DOC systems and environments;
- Lack of funding to modernize legacy systems; and
- Inability to acquire and deploy new technologies rapidly to address emerging threats.

Strategy | DOC's approach to managing identified risk utilizes the FITARA governance process. Mitigations for the risks listed above are outlined below:

- Risks 1 and 2: Risks are actively managed through bureau-specific risk management processes, pending the full roll-out of CDM, Enterprise Continuous Monitoring Operations (ECMO), and Enterprise Security Operations Center (ESOC) capabilities.
- Risk 3: DOC has tasked its Enterprise Shared Services group with developing an Identity Management System as well as other solutions to aid bureaus in their Strong-Authentication/PIV challenges. In the short-term, bureaus are taking actions to address their challenges individually.
- Risk 4: DOC is implementing Federal Cybersecurity Workforce Strategy requirements, and the CIO and Chief Human Capital Officer are establishing an IT workforce development plan. Multiple bureaus also rely on contractor support to address cybersecurity needs.
- Risk 5: Bureaus manage their own vulnerability management programs through a commercially offered, cloud-based platform. Enhanced capabilities will be realized through the roll-out of ECMO, ESOC, and CDM tools. Bureaus employ both risk-acceptance and management strategies.
- Risk 6: DOC continues efforts to develop enterprise-wide contracts for security products; this allow bureaus to quickly acquire new, critical services and manage this risk through the FITARA governance process.

Resources | DOC's cyber posture is continuously reviewed for potential gaps, which are presented to the Departmental Management Council (DMC). DOC's lack of dedicated, real-time enterprise continuous monitoring, including vulnerability and patch management, will be addressed through implementation of ECMO, ESOC, and CDM capabilities and supplemented by bureau-specific processes. Additionally, bureau-level risks and gaps will be addressed by Strong Authentication-related mitigation efforts. Staffing challenges will be addressed through the Cyber Workforce Development initiative. Challenges modernizing legacy systems will be managed at the bureau-level in the short term, though additional investment in modernization efforts is needed. Additional bureau-level gaps include an understanding of enterprise security risks; prioritization of remediation efforts; solutions to mitigate 2020 Decennial Census-related cybersecurity threats; insider threat mitigations; utilization of data loss prevention tools; and full deployment of disaster recovery and business resiliency plans.

Leadership | The DMC, which reports to the Deputy Secretary, is responsible for oversight of DOC's Risk Profile, including the development and implementation of an enterprise-level cybersecurity risk management strategy. Pertinent decision-making is coordinated with budget decisions to provide strategic resource allocation. Within the bureaus, senior leadership is engaged directly in risk management processes through decision-making bodies, regular briefings, and touch-points. Moreover, the ongoing authorization of bureau systems keeps senior leadership apprised of the ever-changing risk environment and actions required to maintain operational and mission success. Through the FITARA governance process, DOC's CIO has enhanced transparency into the IT portfolio and regularly evaluates risks to IT investments.

Inspector General Assessment

The OIG completed an audit of DOC's FISMA compliance by assessing the effectiveness of Commerce's information security program and practices. OIG also reviewed a representative subset of 15 IT systems from four of DOC's operating units to

assess compliance. Overall the OIG determined that the agency does not have an effective information security program.

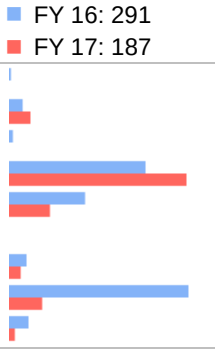
The OIG's assessments of the five functional areas (Identify, Protect, Detect, Respond, and Recover) found that the Department had largely defined needed policies and procedures. Furthermore, the OIG generally found that the metrics related to risk management were consistently implemented and metrics related to security training and incident response were managed and measurable. The OIG did not observe consistent implementation of IT security procedures and practices in configuration management, identity credential and access management, information security continuous monitoring, and contingency planning across the agency.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Education

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	1	0
E-mail	9	14
External/Removable Media	2	0
Improper Usage	89	115
Loss or Theft of Equipment	50	26
Physical Cause	NA	0
Web	11	7
Other	116	21
Multiple Attack Vectors	13	4



CIO Risk Management Self-Assessment

Risks | Strengthening the cybersecurity of the Department of Education's (ED) networks, systems, and data is one of the Department's most critical challenges. Every day, the Federal government experiences increasingly sophisticated and persistent cyber threats. ED's systems house millions of sensitive records on students, their parents, and others, and they facilitate the processing of billions of dollars in education funding. These systems are primarily operated and maintained by contractors and are accessed by thousands of authorized individuals, including ED employees, contractor employees, and other third parties such as school financial aid administrators. Protecting this complex IT infrastructure from constantly changing cyber- threats is an enormous responsibility and challenge.

Strategy | The Department of Education Cybersecurity Strategy and Implementation Plan (ED-CSIP) describes ED's capability gaps as well as related activities to close the gaps and continually develop the Department's cybersecurity program across all of the NIST Cybersecurity Framework functions. ED's strategy for managing identified risks is based on the continued evolution and maturation of the Department's risk management policies, governance, and reporting processes. In its most recent report, from November 2016, ED's OIG noted that the Department had developed a comprehensive governance structure and organization- wide risk management strategy and program that included policies and procedures across ED consistent with OMB policy and applicable NIST guidelines.

Resources | Through activities such as the OIG's annual FISMA audit, ED's continuous monitoring efforts, and DHS's assessments of the Department's HVAs, ED is constantly prioritizing and aligning efforts and resources to address its most pressing issues. ED has accounted for the resources necessary to execute the ED- CSIP in FY 2018 and the out years, but its ability to execute is dependent upon the availability of funding and resources.

Leadership | ED's senior leadership is actively engaged in the development and ongoing implementation of the Department's strategy for cybersecurity risk management. This awareness and support exists at both the strategic and tactical levels. It is informed by threat briefings provided by DHS, and it considers active threats and risks identified through daily security monitoring by ED and DHS.

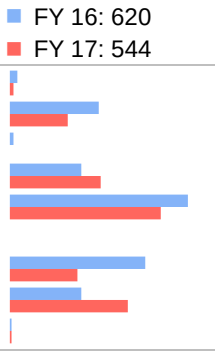
Inspector General Assessment

Based on the maturity model provided in the FY 2017 IG FISMA Metrics, we found the agency was not effective in all five security functions—Identify, Protect, Detect, Respond, and Recover -- wand received an overall rating of not effective. We also identified findings in all seven metric domains: (1) Risk Management; (2) Configuration Management; (3) Identity and Access Management; (4) Security Training; (5) Information Security Continuous Monitoring; (6) Incident Response; and (7) Contingency Planning. At the metric domains level, we determined that the agency's program was consistent with the Defined level of the maturity in Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning, while Risk Management was assessed at the Consistently Implemented level. The FY 2017 maturity model was more comprehensive and attributes were assessed differently than the previous year's maturity model indicator scoring. As a result, certain functions were assessed at a lower level. Despite the lower overall scoring due to changes in the maturity model, we found several areas of improvement from FY 2016. Although the Department made progress in strengthening their information security program, the final report contains recommendations to assist the Department with increasing the effectiveness of their information security program so that they fully comply with all applicable requirements of FISMA, OMB, DHS, and NIST.

FY 2017 Annual Cybersecurity Risk Management Assessment
Department of Energy

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	8	4
E-mail	99	64
External/Removable Media	4	0
Improper Usage	80	102
Loss or Theft of Equipment	197	167
Physical Cause	NA	0
Web	151	75
Other	80	131
Multiple Attack Vectors	1	1



CIO Risk Management Self-Assessment

Risks | DOE faces similar cyber threats to other Federal agencies, including espionage from nation states, advanced persistent threats, and disruptive non-state actors. For DOE, the consequences of a threat actor succeeding could result in damage, disruption, or unauthorized access to business essential and mission critical assets associated with the integrity and safety of personnel, the Nation's nuclear weapons, energy infrastructure, and applied scientific R&D.

A federated and diverse enterprise, DOE is comprised of 97 entities across 27 states with 112 identified HVAs that support its diverse missions. The risk management program is designed with inherent flexibility to mitigate cybersecurity risks to each entity.

Recent internal and external assessments indicate several common risks within the agency, notably below-average management of hardware and software and unauthorized device alerting, as well as a lack of sufficient encryption on some mobile devices. The FY 2017 IG evaluation noted weaknesses in areas such as configuration management, vulnerability and patch management, web application integrity, access controls, continuous monitoring, risk management, and performance monitoring.

Strategy | DOE uses a distributed shared-risk management approach that enables agile identification and acceptance of risk by the appropriate owner. Decisions are primarily driven by the need to mitigate vulnerabilities and impacts and are made in consultation with the CIO and senior agency officials. Information systems that cannot be adequately protected are prioritized for upgrade, replacement, or retirement.

Designated Federal staff accept risk at the local sites based on implementation strategies developed by program offices and informed by DOE policies. Deviation from guidelines at the program or enterprise-level must be documented and accepted at the enterprise-level. When compliance is unrealistic or technically infeasible, controls are prioritized and tailored to mitigate risk. Risk acceptances are reviewed as part of budgetary reviews.

DOE shares information on cybersecurity threats, vulnerabilities, and attack signatures in coordination with the intelligence community and other Federal cybersecurity entities. Known or suspicious activities are shared internally through the integrated Joint Cybersecurity Coordination Center and via automated indicator sharing tools.

Resources | DOE has identified and continues to address the following gaps that contribute to risk:

- Out-dated cybersecurity policies that do not adequately reflect recent Federal mandates.
- Enterprise oversight and visibility into risk management plans and implementation.
- Inconsistent endpoint security controls and vulnerability and configuration management practices.
- Enterprise situational awareness.
- Legacy hardware, software, and systems.

To address these risks, DOE is undertaking efforts to review and update its cybersecurity policy and standard operating procedures. Additionally, the implementation of CDM will provide the visibility needed to address a number of these gaps. DOE is also looking for ways to modernize its critical network architectures, a process complicated by the high interdependence of many of the agency's systems.

Leadership | The Secretary has identified cybersecurity as an agency priority and senior leadership plays an active, influential role in shaping cybersecurity risk management and activities. The CIO provides cybersecurity risk management information to senior leadership, which is included in the Enterprise Risk Profile.

DOE's Risk Management Strategy engages senior leaders to make risk management decisions through the agency's governance model, including numerous boards and forums designed to increase collaboration and allow cybersecurity risks to be examined and evaluated from a department-wide perspective. The DOE Cyber Council, traditionally chaired by the Deputy Secretary, and Information Management Governance Board are used by DOE senior leadership to establish and promulgate risk-informed decisions regarding budget, procurement, personnel, and other investments.

Inspector General Assessment

The OIG conducted the annual evaluation of the DOE's unclassified information security program and obtained results from the agency's Office Enterprise Assessments concerning the agency's national security systems. The OIG reviewed the agency'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 agency was generally effective in implementing a cybersecurity program. While improvements should continue to be made, the OIG found that the agency had Consistently Implemented (Level 3) the following functions: (1) Identify; (2) Protect; (3) Detect; and (4) Recover. The OIG also noted that the Department was at the Managed and Measurable

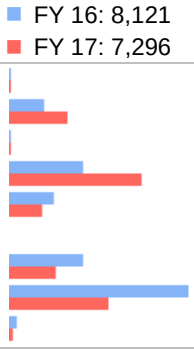
level (Level 4) for the Respond function. Because of the non-homogeneous nature of the agency's population, it is likely that the weaknesses discovered at certain sites reviewed may not be representative of the agency's enterprise as a whole, and the overall results could change from year to year depending on which locations are tested by the OIG.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Health and Human Services

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	6	14
E-mail	693	1,120
External/Removable Media	9	5
Improper Usage	1,445	2,575
Loss or Theft of Equipment	884	651
Physical Cause	NA	0
Web	1,458	907
Other	3,473	1,952
Multiple Attack Vectors	153	72



CIO Risk Management Self-Assessment

Risks | The Department of Health and Human Services (HHS) leverages an ERM approach to implement an enterprise-wide cybersecurity program to protect its critical information. HHS continuously monitors for new risks, prioritizes based on impact, and adjusts remediation and mitigation strategies. HHS efforts have resulted in consistent improvements against milestones and activities identified and measured within various external sources. HHS prioritized four key IT security risks:

HVAs: HHS developed a comprehensive HVA identification methodology and a corresponding evaluation methodology, utilizing a priority-based risk management approach that focuses on the protection of these HVAs.

Legacy IT: HHS routinely assesses risk with technology across the enterprise and determines plans for action and identifies unsupported technologies;

Shared Services and the CDM Program: Gaps in available shared services across government expose agencies to risk, including a lack of cloud brokerage capabilities enabling migration to cloud-based systems in standardized, secure ways with consistent service level agreements, and contract requirements. More critically, DHS' implementation of the CDM program remains behind schedule and affects six (6) CAP Goal metrics;

Cybersecurity Workforce: HHS is focused on building and retaining talent, using available analytics to target and recruit IT professionals that advance HHS' IT competencies. Without significant, ongoing investment in and commitment to people, HHS risks losing a return on technology investments and jeopardizes HHS's ability to effectively protect Americans' health and provide essential human services.

Strategy | HHS developed a department-wide ERM strategic approach which establishes that cybersecurity risks are enterprise issues, coupled with dynamic response mechanisms to respond to emerging risks. This approach is intended to address HHS's four priority risks.

HVAs: HHS conducts ongoing HVA evaluations at Operational Divisions (OPDIVs) leveraging the NIST Cybersecurity Framework;

Legacy IT: HHS identifies unsupported technologies at each OPDIV and defines a roadmap to address these in its HVAs;

Shared Services and CDM: HHS is updating, maintaining, and completing shared services milestones starting with CDM Phase 1 implementation alongside DHS and integrators; and

Cybersecurity Workforce: HHS is focused on acquiring, deploying and sustaining a technology-enabled workforce using strategies such as hiring programs and flexibilities, partnerships with higher education, targeted recruitment, career development, and programs to engage and retain the existing workforce.

Resources | HHS identified three resourcing risks:

Budget: Due to the nature of the annual appropriations process, there is uncertainty in funding HHS's cybersecurity programs.;

Cybersecurity Workforce: As of May 2017, there is a major talent pipeline at HHS; there are 230 vacant information security positions, accounting for 43 percent of the 535 IT job openings. Complicated Federal Government Human Resource processes and legislation, as well as a lack of compensation flexibilities hinder Federal recruitment, hiring, and retention efforts. HHS's IT spend is one of the largest in the government and it needs the IT workforce to support its technology investments;

External Dependencies: The delayed adoption of the DHS CDM Program is the largest single technology risk to HHS's cybersecurity efforts. CDM will provide capabilities that address many of the aforementioned risks.

Leadership | HHS has seen the success of cybersecurity initiatives when they are led by senior department leaders. This includes a 2015 memo outlining cybersecurity priorities and the focus placed on the OMB-driven 2015 Cyber Sprint.

HHS continues to institutionalize cybersecurity as a key priority and is actively advocating the culture shift to treat cybersecurity as an enterprise issue. HHS has established ERM, led by the ERM Council to promote a risk-aware culture across HHS, drive strategic decision via agency risk, and establish and communicate risk appetite. At the same time, HHS continued to engage with senior leadership, including HHS's CIO, Deputy Secretary, and Assistant Secretary for Administration (ASA), on cybersecurity activities, strategies, and risk management. Finally, weekly CIO and Deputy CIO meetings and bi-weekly meetings with the ASA covers cybersecurity critical initiatives, risks, resulting impacts, and requested actions.

Inspector General Assessment

Overall, HHS has made improvements and continues to implement changes to strengthen its enterprise-wide information security program. Based on the results of our evaluation, we determined that HHS' information security program was 'Not Effective' since it was not at a 'Managed and Measurable' level

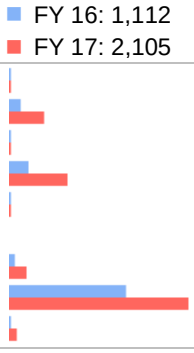
for Identify, Protect, Detect, Respond, and Recover functional areas. HHS is aware of the opportunities to strengthen its overall information security program to ensure that its policies and procedures at all OPDIVs are consistently implemented in all areas of its security program. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS to include continuously monitoring of its networks and systems, documenting OPDIVs' progress to address and implement strategies, and reporting its progress through DHS dashboards. Additionally, HHS needs to makes sure that there is effective vulnerability management, patch management, and access management through the use of appropriate tools and processes at all OPDIVs. These steps will strengthen the program and further enhance the HHS mission.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Homeland Security

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

Incidents by Attack Vector	FY 16	FY 2017
Attrition	1	2
E-mail	79	241
External/Removable Media	18	13
Improper Usage	130	407
Loss or Theft of Equipment	5	16
Physical Cause	NA	0
Web	42	124
Other	818	1,245
Multiple Attack Vectors	19	57



CIO Risk Management Self-Assessment

Risks | Significant portions of the DHS IT infrastructure have aged beyond service life and supportability, impacting both HVAs and Mission Essential Functions. The problem is made worse by a large number of mission-critical IT systems with embedded operating systems that cannot be upgraded and a lack of redundant/fail-over capability for some HVAs and Mission Essential Functions. These, combined with inadequate logging and network visibility, place the delivery of key services at an unacceptable level of risk.

Recruiting and retaining Federal cybersecurity personnel is extremely challenging due to competition from the private sector and other agencies. Funding for contractor services has also become more costly and difficult to procure. As a result, DHS has never achieved full staffing levels for cybersecurity, thereby impacting its ability to meet required cybersecurity targets to support labor intensive activities like system authorizations.

DHS's security operations centers are federated, and some lack required functionality. Visibility into external organizations that are processing sensitive DHS data is also inadequate. In addition, many legacy contracts must be re-negotiated to add security controls and monitoring clauses.

The DHS Insider Threat Program expansion of User Activity Monitoring (UAM) capabilities onto the unclassified network presents a significant risk due to its size, scope expense, and multi-year implementation schedule. DHS accepts the risk of not having full, immediate UAM coverage and will mitigate the risk by using enhanced in-place cyber-defense platforms.

Strategy | The agency's strategy for dealing with its aged infrastructure is to heavily resource infrastructure investment. Systems that cannot be immediately upgraded are isolated from the internet to the greatest extent possible and compensating controls are implemented. Additional strategies include budgeting for technology refresh on a not-to-exceed five-year cycle and moving to the cloud. Infrastructure investments to ensure that HVAs and Mission Essential Functions have the required reconstitution capabilities are being elevated within the agency.

The agency is spearheading a two-part approach to better recruit and retain highly skilled cybersecurity personnel: 1) create a program that supports pay incentives and 2) develop an innovative approach that provides a lasting solution to a variety of cybersecurity workforce-management challenges.

Capability gaps within the agency's SOCs and options for remediating them are being evaluated by leadership, including consolidation and utilization of external partner capabilities. Existing contracts, as appropriate, are also being reviewed and amended.

Resources | Overall, the resiliency of the agency's HVAs and Mission Essential Functions must be improved. DHS's largest gap is outdated infrastructure, which the agency seeks to address by moving to a not-to-exceed five-year technology refresh cycle. DHS also seeks to procure scanning tools and technically trained cybersecurity personnel; however, all of these efforts currently face significant budget constraints, and DHS is working to identify funding options. Additional budgetary resources will be needed to execute upon the agency's workforce enhancement strategy. DHS's SOC consolidation efforts should address gaps in security tools and redundancy, but it will not address personnel shortages or the increasing cost of cybersecurity services.

Leadership | DHS leadership, utilizing an internal scorecard, regularly meets with component senior leadership regarding enterprise cybersecurity risk. Additionally the agency has created a cybersecurity maturity model to inform funding decisions and appropriation requests. The DHS's Cybersecurity Performance Plan guides these decisions and its resulting monthly scorecard.

DHS senior leadership, including the Acting Undersecretary for Management, the Undersecretary of Intelligence & Analysis, and the DHS Chief Security Officer, is regularly briefed on the status of the ITP.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. In three of five areas, DHS fell one level below the targeted "Level 4" defined in the FY 2017FISMA reporting guidance as achieving effectiveness in information security. The DHS CISO is centrally responsible for coordinating with other senior agency officials to manage the Department's information security program for its unclassified and national security systems. Based on this year's FISMA results, additional oversight is needed for the agency to improve in ensuring that components comply with Federal and DHS information security policy. Specifically, since the agency's inception in 2003, components have not effectively managed and secured their information systems. Components have continued to operate systems without Authorization to Operate, used unsupported operating systems that expose DHS data to unnecessary risks, ineffectively managed the Plans of Action and Milestones process to mitigate identified security weaknesses, and failed to apply security patches in a timely manner. Such

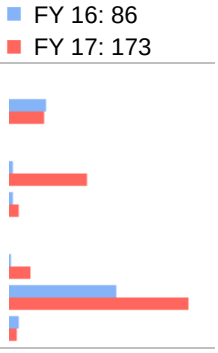
repeated deficiencies are contrary to the President's Cybersecurity Executive Order and are clear indicators that departmental oversight of the enterprise-wide information security program needs to be strengthened. Until DHS overcomes challenges to addressing its systemic information security weaknesses, it will remain unable to ensure that its information systems adequately protect the sensitive data it stores and processes.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Housing and Urban Development

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	20	18
External/Removable Media	0	0
Improper Usage	2	41
Loss or Theft of Equipment	2	5
Physical Cause	NA	0
Web	1	11
Other	56	94
Multiple Attack Vectors	5	4



CIO Risk Management Self-Assessment

Risks | From September 2014 to March 2016 Housing and Urban Development (HUD) performed a current state analysis, including an examination of HVAs and mission essential systems and functions, and determined that HUD needs improvement in 35% of the NIST Cybersecurity Framework controls and identified 11 program areas of concern.

Strategy | Currently, IT security and cybersecurity risks are included within the broader risk management program taxonomy and scope. Following the aforementioned analysis of the agency's cybersecurity posture, HUD began implementation of the NIST Cybersecurity Framework. Additionally, FY 2017 was the first year of the ERM Program at HUD and the organization is in the process of establishing a baseline for current risk activities across the organization.

Resources | HUD assessed that it needs to improve 35% of NIST Cybersecurity Framework controls and developed a strategic plan, organized around the FISMA program areas, to prioritize the gaps that must be addressed most immediately.

Leadership | The Chief Operating Officer and Chief Risk Officer for HUD lead the agency's ERM activities. Currently, IT security and cyber risks are included within the broader risk management program taxonomy and scope, and the Chief Operating Officer and Chief Risk Officer will be working with CIO leadership to address the requirements regarding cybersecurity risk management.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. Long-standing core issues continue to challenge HUD and place significant limitations on the CIO's ability to establish an effective information security program. HUD has not yet matured its risk management program and other program components, such as continuous monitoring and incident response, and thus HUD lacks the foundation to make risk-informed decisions. Continuous turnover and vacancies in key IT leadership positions make it difficult for HUD to establish continuity when determining its priorities and implementing its processes. Reduced funding levels for IT and cybersecurity restrict HUD's ability to implement sufficient technology to properly secure and monitor its data and modernize its numerous legacy systems. Extensive reliance on contracting and lack of mature metrics prevent HUD from conducting proper oversight of contractor cybersecurity activities to ensure that HUD systems and data are adequately protected.

Notable HUD initiatives include the rollout and refinement of its new incident response capability, the deployment of solutions to enhance its threat detection and network monitoring capabilities, and the initiation of enterprise and OCIO risk management programs. HUD continues to work closely with DHS to leverage the capabilities provided by DHS for intrusion detection and prevention.

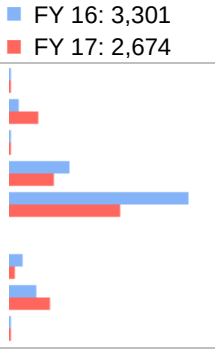
The OIG recommends that HUD strengthen its oversight across the agency to ensure consistent implementation of its IT and cybersecurity policies and procedures, fully mature its risk management and continuous monitoring programs, and assess the adequacy of funding and human capital planning applied to the information security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Justice

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	1	6
E-mail	119	339
External/Removable Media	3	1
Improper Usage	685	513
Loss or Theft of Equipment	2,022	1,267
Physical Cause	NA	0
Web	144	61
Other	313	457
Multiple Attack Vectors	14	30



CIO Risk Management Self-Assessment

Risks | The Department of Justice (DOJ) utilizes its ERM process to identify risks at the strategic, operational, reporting, and compliance levels. DOJ regularly reassesses and reprioritizes identified and new risks. DOJ and external organizations perform security reviews at the agency, component, mission, and system level, assessing the risk posture and security program implementation of DOJ. DOJ improves the cybersecurity posture of its networks and systems by using the results of these reviews to prioritize actionable steps to reduce residual risk in DOJ's information and information systems.

Strategy | DOJ utilizes a three-tiered risk management approach as described in the NIST SP 800-37. DOJ's tiers are the information system, component, and DOJ. DOJ utilizes risk management systems including the Cyber Security Assessment and Management application for all security assessment and authorization data and the Security Posture Dashboard Report, allowing DOJ to measure asset, vulnerability, and configuration data. SPDR calculates a risk score for at all tiers, ensuring leadership is aware of DOJ's risk posture. Using these tools, DOJ is able to manage identified technical risks at all three tiers in an effective manner. DOJ seeks to mitigate and eliminate risk through the careful application of cybersecurity protections in the form of procedural or technical implementations.

Resources | DOJ regularly evaluates solutions to all identified risks and prioritizes efforts and resources to ensure their timely remediation. DOJ is taking steps to enhance its cybersecurity program as it prepares to leverage IT shared services and migrate systems to the cloud. DOJ is also working with its human resource staff to understand the cyber talent market and decrease recruitment time.

Leadership | DOJ senior leadership is regularly involved in risk identification, prioritization, and remediation as part of the risk management strategy. DOJ leadership attends a monthly Cybersecurity Committee and CIO Council in which a heat map of Components' cyber risk scores is presented, resulting in friendly competition to achieve the lowest score. The DOJ CIO meets with the Office of the Deputy Attorney General on a weekly basis, ensuring leadership is aware of cybersecurity priorities. Senior leadership prioritizes risk remediation and works with budget officials for increased funding.

Inspector General Assessment

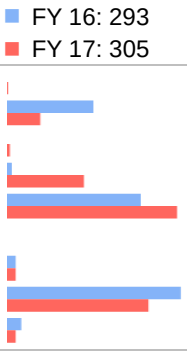
During FY 2017, the DOJ OIG reviewed the information security programs of six DOJ components and a sample of 14 systems within these components. The OIG determined that the maturity level for DOJ's information security program is "Level 3 – Consistently Implemented" across all five NIST Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. While the OIG determined that DOJ is effective in one of the five security functions, Respond, the OIG determined that the DOJ's overall information security program is not effective due to the exceptions noted within the other four functions. The OIG made recommendations to address DOJ's program in the Risk Management, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, and Contingency Planning domains to enhance the effectiveness of DOJ's information security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Labor

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	60	23
External/Removable Media	0	2
Improper Usage	4	53
Loss or Theft of Equipment	92	117
Physical Cause	NA	0
Web	7	6
Other	119	97
Multiple Attack Vectors	11	6



CIO Risk Management Self-Assessment

Risks | The Department of Labor's (DOL) OCIO Enterprise Risk Management Strategy (ERMS) program provides rigorous review processes for the identification, assessment, and prioritized risk mitigation and remediation for its HVAs and systems that support its Mission Essential Functions. Risks identified via independent assessments are also managed via DOL's ERMS program. These have resulted in the following priority risks:

1. Asset Management: DOL's limited ability to identify and immediately remove unauthorized devices attempting to connect to DOL's network increases the risk of system compromise;
2. Access Management: Disparate technologies and manual access management processes continue to present a potential risk of unauthorized access due to delayed removal of access for separated employees and excessive elevated privileges; and
3. Security Operations Monitoring and Incident Management Capabilities: Limited resources impact DOL's ability to monitor its operating environment and manage security incidents. These resource limitations contribute to delays in DOL's Enterprise Security Operations Center's (ESOC) response to and recovery from incidents.

Strategy | DOL's strategy leverages the ERMS program and the NIST standards to identify gaps and provide a holistic approach that includes periodic assessments and continuous monitoring. The Department prioritized these capabilities based on the presence of PII. The resulting risk remediation activities are as follows:

1. Asset Management: DOL has prioritized mitigating the risk of unauthorized devices connecting to the network. It is in the process of implementing capabilities to detect unauthorized connections to reduce the risk;
2. Decentralized Access Control: In FY 2017, DOL acquired a suite of tools to give it the ability to implement an enterprise identity and access management solution targeted for implementation in Q2 of FY 2018; and
3. Security Operations Monitoring and Incident Management Capabilities: In FY 2017, DOL implemented web content filtering and detonation chamber for emails. DOL also began implementation of a Security Information and Event Management capability and other critical ESOC capabilities. The SIEM capability is planned for completion at the end of FY 2018.

Resources | Mission impact has been taken into account as DOL has aligned resources to address capability gaps. Specifically, cybersecurity program budget increases allowed the hiring of Federal and contractor resources. DOL also expedited acquisition processes to procure critical security tools. Specific efforts include:

1. Asset Management: DOL has been working to align the various DOL stakeholders related to budget, tools, people, and processes. Additional funding will be required to acquire an enterprise asset management solution;
2. Decentralized Access Control: Integrating the Department's legacy applications with DOL's enterprise IAM solution poses a significant challenge due to outdated and/or unsupported application code. Additional funding, tools, and people will be needed to modernize and integrate the applications; and
3. Security Operations Monitoring and Incident Management Capabilities: Implementation of additional ESOC tools will require continued upgrades to DOL's infrastructure. In addition, implementing DOL's SIEM solution requires an upgrade of its computing and storage to store the increased amount of log information.

Leadership | Senior leadership plays a critical role in the development and ongoing implementation of the DOL cybersecurity risk management strategy. The Senior ERM Team, which consists of the Deputy Secretary, CIO, Deputy Assistant Secretary for Operations, and CISO, is responsible for overseeing DOL's IT risk management strategy and activities and ensuring the cybersecurity risk management strategy integrates with the DOL ERMS. Areas that require management risk decisions are documented as part of the ERMS risk acceptance and exemption process. Results require DOL agency-level and OCIO executive -level approval and signature.

Inspector General Assessment

The purpose of the DOL OIG evaluation was to determine if DOL implemented an effective information security program for the period October 1, 2016, to September 30, 2017, in addition to assessing DOL's compliance with FISMA and information security policies, procedures, standards, and guidelines. The

OIG determined that DOL's information security program was not effective during this period.

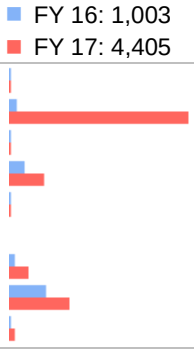
The determination was based on testing of a selection of enterprise-wide information security program controls and a selection of system-specific security controls across 20 information systems. The OIG reported 33 findings in four security control areas, encompassing identity and access management, incident response, contingency planning, and configuration management and made recommendations to the CIO for remediation. Recommendations for the CIO included conducting a sufficient risk assessment to identify the root causes of the identified deficiencies; documenting, tracking, and implementing milestones and corrective actions to timely remediate identified deficiencies conveyed to DOL management; coordinating efforts among DOL components to design and implement procedures and controls to address account management, system access settings, configuration management, system audit log configuration and reviews, and patching and vulnerability management control deficiencies in key financial feeder systems; and monitor the components' progress to ensure that established procedures and controls are operating effectively and maintained.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of State

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	1	8
E-mail	116	2,598
External/Removable Media	1	8
Improper Usage	240	525
Loss or Theft of Equipment	2	27
Physical Cause	NA	0
Web	89	281
Other	543	877
Multiple Attack Vectors	11	81



CIO Risk Management Self-Assessment

Risks | The Department of State's (State's) extensive global footprint and diverse mission present unique challenges for managing cybersecurity. State faces persistent threats, and the agency is a target of interest from nation states, criminals, and hacktivists. Adversaries are exploiting the speed, convenience, and anonymity of the Internet to launch millions of attempts to breach State's networks annually.

State has 572 systems supporting mission essential functions and programs, including 11 HVAs. The targets of most concern are those with human resource, financial, investigative, consular, and medical information, as well as correspondence between key leaders. Threat actors seek access to these assets to expose the agency to physical harm, to cause political embarrassment, and to damage national interests.

The risk to State is high given the prevalence of threat actors and the impact of a potential exploitation of the agency's mission.

Strategy | State leverages business rules designed to minimize agency risk. State does not recommend accepting risk for systems with any high or a series of moderate weaknesses. When exceptions are granted due to operational need, the period of authorization is short and remediation is monitored. Efforts are underway to further refine and prioritize technical and programmatic risk treatments. This includes increasing the transparency of IT investment costs and functionality and ensuring cybersecurity efforts are appropriately reflected.

State compensates for persistent risks through a series of measures. The agency operates a mosaic of perimeter capabilities and a continuous monitoring program to compensate for its large backlog of system security authorizations. For systems not hosted on Open-Net networks and that do not offer the same security protections as Open-Net, State is inventorying the systems in preparation for further assessment. Due to the prevalence of phishing attacks, State also employs phishing exercises to educate users and reduce the likelihood of a successful attack.

Resources | The informed decision making needed to make risk prioritization choices on security authorizations has been negatively impacted by staffing shortages. State continues to work with Federal and industry partners to utilize mechanisms such as rotational assignments and skills development programs to develop and better retain skilled staff. Additionally, State has workforce partnerships in place with DHS, NSA, the Marine Corps, and others; however, the Executive Order on government reorganization has impacted the targets and milestones across all offices.

Process gaps also persist. State plans to make use of automation through DHS' CDM program to decrease the time and expense of authorization processes; however, implementation delays and staffing shortages have limited its utility.

Legacy technology and outdated architecture also present challenges. State is modernizing major systems and applications and segmenting enterprise architecture while reducing the variety of supported technologies. This is a multi-year effort directly affected by available funding and staffing.

Leadership | The CIO manages cybersecurity risk for State, advising senior leadership on IT security issues and implementing resulting directives. This includes overseeing the Cybersecurity Steering Committee and participating in and advising the agency's Management Control Steering Committee. The CIO sits on the ERM Council and chairs the executive-level IT Investment Review Board, reviewing the health, value, security, and risk for all IT investments across State. The CIO has direct input into budget submissions on all IT-related funding issues, acquisition plans, and actions.

The CIO meets bi-weekly with various bureau leads and as needed with the Deputy Secretary to discuss cybersecurity issues. The CIO established the role of Enterprise Risk Officer for Cyber in November of 2016 and announced his intent to increase the emphasis on risk management.

Inspector General Assessment

The private firm auditing the agency's information security program and practices concluded it has not realized an effective organization-wide information security program. Five recommendations were provided to improve the agency's information security program, including elevating the organizational placement of the CIO, implementing an information security risk management strategy, and identifying and maintaining an accurate inventory of information systems.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of State Office of Inspector General

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Optimized
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover	Managing Risk	Optimized

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Department of State 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. In addition, future budget constraints and hiring restrictions could affect the OIG's ability to effectively monitor and protect its network. OIG has also migrated to OIGNet, an independent network, and underwent an independent assessment by a FedRAMP-certified third party assessment organization.

Strategy | In the earliest planning and design stages of OIGNet, OIG integrated security engineering principles to develop a layered, defense-in-depth architecture and security requirements across all life-cycle planning phases. OIG mapped cybersecurity requirements and best practices to security features, capabilities, and tools commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of OIG data. OIG also implemented the NIST RMF. OIG's risk response includes acceptance, avoidance, reduction, or sharing. Risks that the agency cannot fully remediate require mitigation and residual risk acceptance by the OIG Authorizing Official

Resources | OIG identified potential gaps in phishing awareness, vulnerability tracking, and overseas travel mobile security. OIG has since aligned budgetary resources and procured solutions to address the identified gaps. OIG procured a platform to conduct both regular phishing campaigns and security awareness training. In addition, OIG procured a technical solution to track system vulnerabilities centrally by age to improve overall vulnerability management.

Leadership | OIG senior leadership plays an integral role in cybersecurity risk management and in the broader ERM process. OIG conducts cybersecurity risk assessments utilizing a variety of tools and processes, assigning identified risks to an owner and tracking them centrally until addressed. The CISO apprises OIG senior leadership of risks and assessment results through weekly metrics reporting, monthly project status meetings, and strategic plan performance reviews and reporting. OIG senior leadership sets priorities and allocates funding for cybersecurity and other programs and projects based on alignment to mission essential functions, compliance requirements, and program evaluations results, which include cyber security continuous monitoring.

Inspector General Assessment

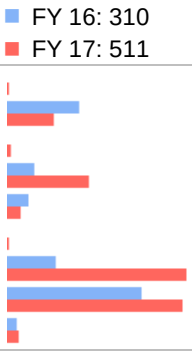
The OIG's independent auditors determined that the office has an effective information security program. The auditors found no significant deficiencies and found that success of OIG's information security continuous monitoring and cybersecurity practice was based on providing sufficient people, processes, resources, and technology; adequate both in amount and kind. The auditor found effective practices supported by concrete evidence, demonstrating optimization and continuous improvement in virtually all process areas. The auditor notes that the cybersecurity practices at OIG are demonstrably sustainable.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of the Interior

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	2
E-mail	71	47
External/Removable Media	0	4
Improper Usage	26	81
Loss or Theft of Equipment	22	14
Physical Cause	NA	2
Web	49	176
Other	133	173
Multiple Attack Vectors	9	12



CIO Risk Management Self-Assessment

Risks | The Department of the Interior's (Interior) mission-critical systems were not designed for today's cyber threats. Infrastructure add-ons and system upgrades only extend system mission life and do not drastically improve IT security. Outdated IT systems also increase the risk of malicious actions resulting in the exfiltration of controlled unclassified information, compromised integrity, and mission availability. Interior's decentralized service model also presents challenges, including inefficient spending, poor interoperability, limited visibility, and localized architectures that add significant cybersecurity risk. If realized, such compromises could cause loss of life and financial harm to the American people.

Acceptable Use Policies also represent a risk; they do not effectively balance mission risk and employee convenience and are often exploited to gain access to data and systems. Countermeasures and remediation costs are high with limited effect. Human errors also expose networks and systems to exploits. Updating policy regarding the secure use of personal smart devices could result in additional resources that could be reinvested elsewhere.

Overall, Interior needs new enterprise architectures and service models for the tomorrow's cyber environment.

Strategy | The CIO selectively delegates the role of Authorizing Official to specific management officials across the agency systems to assume authority over cybersecurity risks based on their functional, management, and financial authority over information systems. These officials make risk-based determinations for the system authorization boundaries under their purview. The CIO, typically in consultation with the agency's senior leadership, then decides how to manage the risks based on the severity of impact on the agency and the likelihood of occurrence.

In terms of specific strategic policy direction, Interior's Chief Technology Officer is finalizing a technical guide on applying micro-segmentation strategies for HVAs, which could mitigate the collateral risk of a single incident by making lateral movement across a network more difficult. In addition, the CIO will issue formal guidance to HVA owners and their technical staff on necessary actions.

Resources | Interior's highest-priority cybersecurity gaps are:

- Implementation of secure access and strong authentication for non-Windows based HVAs at the network and application levels;
- Sustainment of the DHS initial investment in the CDM program tools implemented in 2015 that provide Interior with the ability to detect and respond to malicious activity on the network in a timely manner;
- Strengthening of internal network protection from cyberattacks on publicly-facing systems; and
- Implementation of additional data protections for HVAs, many of which are mission-critical systems that support Interior's core mission. In addition, mission-critical systems continue to age, presenting challenges to the adoption of modern, innovative approaches to doing business.

Interior will leverage the CDM program to acquire tools for secure access and strong authentication (CDM Phase 2), and to sustain operations and maintenance for the capabilities implemented in CDM Phase 1. In 2019, the CDM program will be funded internally as a mandatory initiative through the Department's Working Capital Fund. The CIO is working with bureau information management and technology leaders to re-examine its approach to prioritization and use of internal resources to meet Interior's goals.

Leadership | Interior's ERM practice leans heavily on the CIO, leaders from the Assistant Secretary - Policy, Management and Budget's office, and the Deputy Solicitor for General Law for legal counsel. The CIO is the IT Risk Executive Officer and Senior Accountable Official for Risk Management and reports directly to the Secretary.

The CIO reviews cybersecurity risk with senior leadership biweekly. Senior leadership lends support to the CIO in pursuing risk mitigation and risk management opportunities. Senior leadership also reviews cybersecurity capability gaps and supports budget requests to close identified gaps. The CIO maintains final authority for information and system risks in the Department.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. A Performance Audit was conducted over the information security program and practices of the Department of the Interior to determine the effectiveness of such programs and practice for the FY ending September 30, 2017. The scope of the audit included the following Bureaus and Offices:

- Bureau of Indian Affairs, Bureau of Land Management, Bureau of Ocean and Energy Management, Bureau of Reclamation, Bureau of Safety and Environmental Enforcement, U.S. Fish and Wildlife Service, Interior Business Center, National Park Service, OIG, Office of Natural Resources Revenue, Office of the Secretary, Office of Surface Mining Reclamation and Enforcement, Office of the Special Trustee for American Indians, Office of the Solicitor, and U.S. Geological Survey.

Interior had 125 operational unclassified information systems and 15 information systems were randomly selected for the audit. Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST's standards and guidelines, Interior established and maintained its information security program and practices in the five NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, and Recover).

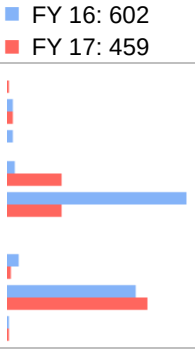
However, the Interior's cybersecurity program was not fully effective as deficiencies were identified in each Cybersecurity function area. Deficiencies were noted in the FISMA domain areas of risk management, configuration management, information security continuous monitoring, incident response, and contingency planning metric domains.

Consistent with the FY 2017 OIG FISMA metric rating instructions, ratings throughout the seven FISMA domains were identified by a simple majority, where the most frequent level across the FISMA metrics served as the domain rating. The independent auditor assessed the NIST Cybersecurity Framework function areas of Identify, Protect, Detect and Recover as Consistently Implemented (Level 3) and the Respond function as Defined (Level 2). Overall, Interior was assessed at Consistently Implemented (Level 3).

FY 2017 Annual Cybersecurity Risk Management Assessment
Department of the Treasury

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	10	10
External/Removable Media	10	0
Improper Usage	15	95
Loss or Theft of Equipment	315	95
Physical Cause	NA	0
Web	22	8
Other	226	248
Multiple Attack Vectors	4	2



CIO Risk Management Self-Assessment

Risks | In addition to cybersecurity risks common to all complex organizations, the Department faces specialized risks. Namely, the Department must adapt to manage an evolving cyber threat landscape while also maintaining the integrity of financial market data, sustaining payment processing systems, upholding the confidentiality of personally identifiable information, and preserving the secrecy of policy analyses. IT is highly integrated into the business processes that support these functions, especially in the areas of tax administration, debt operations, payment processing, and fiscal policy.

Leveraging the NIST Cybersecurity Framework, Treasury assesses cybersecurity risk at the enterprise, mission-area, program, and system levels. The Department considers a wide range of inputs to assess its cybersecurity risk, including the results of compliance-driven audits, assessment of intelligence, and metrics. While cybersecurity risk at the bureau level varies, the Department is largely meeting government-wide security targets.

Treasury is working to extend application of the NIST Cybersecurity Framework to the system level, starting with mission-critical high-value assets. Treasury seeks to create a cascading assessment mechanism to achieve and sustain an acceptable level of risk across the portfolio of systems.

Strategy | Treasury employs a risk-based approach to cybersecurity, comparing the likelihood of a risk being exploited to its impact. Once Treasury identifies a known risk, it administers a network defense by employing rapid application of hardware and software patches and adjusting access control policies. To reduce the impact of exploitation, Treasury operates comprehensive data logging and analytics and data loss prevention platforms. It also encrypts data in-motion and at-rest. Treasury routinely tests these capabilities to confirm their efficacy.

In situations where these measures cannot adequately reduce the likelihood or impact of exploitation, Treasury makes risk-based decisions based on a defined risk evaluation process.

Resources | One of Treasury's most significant cybersecurity risks is the theft of sensitive data and financial fraud executed through tax and payment systems. This risk is exacerbated by Treasury's use of legacy IT, which is often incompatible with modern risk mitigation solutions.

In order to address these gaps, Treasury needs a more robust network defense; a stronger authentication system utilizing multiple factors; a data loss prevention platform; and enhancement to its incident response and recovery processes.

With these needs in mind, in FY 2017 Treasury submitted a budget request and Congress appropriated fund for a Cyber Enhancement Account directly tied to the requirements outlined above. Treasury has begun allocating those funds to acquire enhancements to a DLP platform; a platform that performs behavioral analysis on malware; platforms to decrypt inbound and outbound encrypted network traffic; and forensic tools to automate incident response and recovery processes.

Enterprise technologies alone will not fully address the highest priority risks. Treasury will also implement stronger, more centralized cybersecurity governance; develop policies and procedures to institutionalize response and recovery processes; conduct annual exercises of disaster and incident response plans; and test network defense capabilities annually. Treasury is also building an internal team of experts who can supplement third-party security assessments to identify emerging threats.

Leadership | The Secretary of the Treasury is committed to cybersecurity as one of his highest priorities and has been directly involved in the formulation and execution of Treasury's approach to cybersecurity, inside and outside the agency. He is briefed monthly on all components of Treasury's cybersecurity equities, including risks facing the international community, financial sector, and Treasury's internal systems.

The Acting Deputy Secretary of the Treasury has oversight of cybersecurity across the Department. He attends monthly meetings with the Assistant Secretary for Management and Treasury's CIO and CISO to discuss the overall health of the Department's internal cybersecurity program. These briefings include review of the Department's performance against government-wide targets, as well as the status of specific security controls and cyber protection programs.

The Office of the CIO and the Office of the Chief Risk Officer work closely to integrate cybersecurity into ERM practices. The CIO participates in monthly meetings with the Chief Risk Officer and other senior-level officials to review the risk landscape. The Chief Risk Officer routinely participates in the risk review of high-value assets.

Inspector General Assessment

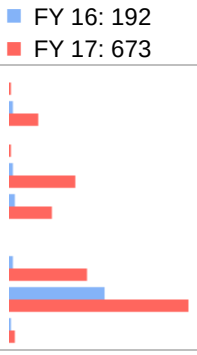
Consistent with applicable FISMA requirements, OOMB policy and guidance, and NIST standards and guidelines, Treasury's information security program and practices for its unclassified

systems were established and have been maintained for the five NIST Cybersecurity Framework functions and the eight FISMA program areas. However, a total of seven deficiencies were found within three of the functions and four of the FISMA program areas. With respect to IRS's unclassified systems, Treasury IG for Tax Administration (TIGTA) reported that Internal Revenue Service's (IRS's) information security program generally aligned with applicable FISMA requirements, OMB policy and guidance, and the NIST standards and guidelines. However, due to program attributes not yet implemented, IRS's information security program was not fully effective. TIGTA found that three security program areas failed to meet FISMA requirements overall. Lastly, consistent with applicable FISMA requirements, OMB policy, CNSS policy and guidance and NIST standards and guidelines, Treasury established and maintained its information security program and practices for its collateral national security systems for the five functions and the eight FISMA program areas. However, there were four deficiencies identified within three of the functions and four of the FISMA program areas.

FY 2017 Annual Cybersecurity Risk Management Assessment
Department of Transportation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	8	49
External/Removable Media	0	3
Improper Usage	7	111
Loss or Theft of Equipment	9	71
Physical Cause	NA	0
Web	5	130
Other	160	297
Multiple Attack Vectors	3	11



CIO Risk Management Self-Assessment

Risks | The Department of Transportation's (DOT) systemic and programmatic risks include:

- Limited integration of cyber and privacy risk management into the management of IT investments and the systems development lifecycle;
- Insufficient personnel to manage cybersecurity compliance and assess risk for systems within its inventory and investment portfolio and to fully implement its Information Security Continuous Monitoring strategy
- Underinvestment in cybersecurity with significant dependencies on shared services that operate at "continuing services" levels without large reserves for risk mitigation and modernization;
- Lack of a consolidated, enterprise-wide view of cybersecurity risk resulting from disaggregated tools, underutilization of an existing risk-management-framework/governance-risk-compliance platform, and policy and authorities issues that complicate information sharing and oversight activities; and
- Lack of updates to Mission Essential Functions inventory, resulting in gaps and uncertainties.

Other significant risks include:

- The common operating environment is in need of modernization, has end-of-life hardware and insecure configurations, is not as resilient as required, and does not provide for full segregation of systems/assets;
- A large percentage of agency systems do not yet leverage PIV credentials for strong authentication; and
- The agency has not yet completed deployment of the DHS' CDM program capabilities.

Strategy | DOT executes the cybersecurity strategy and approach for managing risk at the enterprise, mission/business, and system levels, and leverage a variety of internal and independent external assessment tools. At the enterprise level, DOT has established a committee under the agency CIO Council, and the Federal Aviation Administration (FAA) established an internal steering committee. There is also a regular review of agency-wide High Value Risk/High Value Threats to assure consistent risk acceptance decisions and provide direction on mitigation actions.

At the mission/business level, component processes support local risk management activities, and cross-organizational communications facilitate collaboration and information sharing to ensure alignment with DOT priorities. Individual authorizing officials are empowered to accept and fully manage and mitigate risks, while component CIOs are accountable for component-level IT oversight, assessment, categorization, and management of risk.

Resources | DOT is implementing its Cybersecurity Workforce Management Program to ensure: 1) talented cybersecurity professionals are hired, properly trained; and 2) contract staff working on cybersecurity are inventoried and properly trained. The DOT OCIO is working with the DOT CFO and others to establish a roadmap for future staffing needs. Additionally, DOT and FAA processes are designed to assure a consistent and cohesive operation of the organization based on our safety mission.

To further address resource gaps, DOT and FAA conduct budgetary reviews to identify evolving needs and ensure resources are appropriately aligned to address mission needs and identify where deficiencies exist.

Leadership | The DOT CIO is the principle interface between the agency's cybersecurity risk management program and senior leadership. Senior leadership is responsible for affirming strategies and plans presented by the CIO, communicating adjustments in priorities, providing supportive messaging to internal executives, and communicating needs and concerns to OMB and other elements of the Administration.

Most cybersecurity risk is managed through collaboration between the CIO, CFO, and Chief Acquisition Officer, which includes reviewing IT budgets, spend, investments, and acquisitions to ensure proper management of various programmatic and security risks. The Department OCIO also uses that information to support the formulation of future budgetary requirements, and direction to Component CIOs on IT priorities.

Inspector General Assessment

DOT's information security program is not effective. We tested a statistical sample of 45 of 464 systems, data extracted from DOT's FISMA reporting system and data supplied from its components (e.g., FAA) and the CIO's office. Our assessment covered the 12-month period ending June 30, 2017. We also discussed our observations with DOT and its components. In general, DOT updated its policies, procedures and processes to meet the criteria set forth in the OMB/DHS's FISMA metrics for OIGs. However, DOT was not successful in consistently implementing these policies or procedures. Of note, at least 70 systems have been identified that have not been authorized to operate, over 1300 high/medium-priority plans of actions and

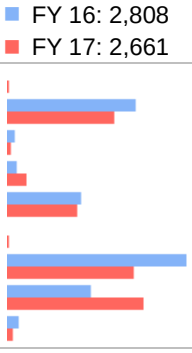
milestones have no planned start date, over 200 systems are not PIV enabled, and inventories of hardware and software are unreliable or unavailable. Our testing of sample systems also revealed that the majority of the systems had controls that were not effectively monitored on an ongoing basis, configuration related weaknesses, and had contingency planning and testing issues, among other things. A number of these and other weaknesses have been previously identified. For example, in 2016 we noted that DOT's incident reporting operations center did not have access to departmental systems to monitor them for security incidents. This weakness persists. DOT's cyber security program is not effective.

FY 2017 Annual Cybersecurity Risk Management Assessment

Department of Veterans Affairs

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	731	614
External/Removable Media	49	19
Improper Usage	53	107
Loss or Theft of Equipment	419	394
Physical Cause	NA	2
Web	1,015	723
Other	472	771
Multiple Attack Vectors	69	30



CIO Risk Management Self-Assessment

Risks | The Department of Veterans Affairs (VA) operates a robust enterprise-wide RMF program that is fully aligned with NIST guidelines. As part of this program, VA monitors and manages system-specific risks through agency plan of action and milestone processes. VA also proactively manages cybersecurity risks to its HVAs and Mission Essential Functions by leveraging the DHS to perform a RVAs on these systems.

Strategy | VA's agency-wide RMF standardizes the organizational management of identified risks. The RMF provides VA with the ability to assess compliance, measure operational risk, and ultimately make risk-based determinations for an information system's Authority to Operate. VA monitors risks to information systems via a Governance, Risk, and Compliance tool, and makes strategic and operational decisions to determine whether to accept, transfer, or mitigate the risk. VA considers budgetary factors in concert with mission criticality when determining whether to accept, transfer, or mitigate the risk.

The CIO tracks the progress of activities to remediate OIG FISMA audit findings, address additional gaps, and identify capabilities to resolve the highest priority risks. Additionally, VA continues to actively engage DHS and the OMB on a regular basis to discuss the status of ongoing cybersecurity activities, which assist the Department in addressing cybersecurity capability gaps.

Resources | VA is well positioned to resolve high impact potential risks to the Department through existing Enterprise Cybersecurity Strategy Program (ECSP) initiatives, which address tactical and strategic cybersecurity-related actions. VA performs comprehensive reviews of the ECSP and underlying domains to better understand the resources required to execute the tactical and strategic activities. As part of VA's ongoing ECSP refresh, the agency will use risk-based metrics to prioritize remediation efforts, allocate resources, and address risks to secure VA mission and business processes.

Leadership | VA senior leadership plays a direct and persistent role in the implementation of VA's cybersecurity risk management strategy and ongoing integration efforts across the enterprise. This direct engagement provides VA leadership with a continual understanding of VA's cybersecurity risks, enabling informed decisions to reduce overall risk to the Department. VA uses the ECSP reporting processes to provide VA executive leadership with a centralized and transparent view of VA cybersecurity projects and initiatives. VA continues to enhance its existing cybersecurity risk management strategy by integrating the RMF with the Cybersecurity Framework to provide executive-level visibility into cybersecurity risk at the system and Department levels.

Inspector General Assessment

The OIG determined through independent review that the agency has does not have an effective information security program. The VA OIG assessed VA's information security program through inquiries, observations, and tests of selected controls supporting major applications and general support systems at 24 VA facilities. The OIG found that, while VA has made progress developing cybersecurity policies and procedures, it still faces challenges implementing components of its agency-wide information security continuous monitoring and risk management program to meet FISMA requirements. While some improvements were noted, this audit identified continuing significant deficiencies related to access controls, configuration management controls, continuous monitoring controls, and service continuity practices designed to protect mission-critical systems. Weaknesses in access and configuration management controls resulted from VA not fully implementing security standards on all servers, databases, and network devices. VA also has not effectively implemented procedures to identify and remediate system security vulnerabilities on network devices, databases, and server platforms VA-wide.

FY 2017 Annual Cybersecurity Risk Management Assessment

Election Assistance Commission

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Election Assistance Commission (EAC) is an extremely small agency but serves in one of the highest profile segments of the country—election administrators in more than 8,000 jurisdictions. These administrators count on the EAC to share timely and relevant information and best practices, certify voting systems to accepted standards, and to collect and distribute relevant information from a semi-annual administration survey. The EAC manages limited physical assets. From a cyber-security standpoint, EAC's risks are mitigated by having most IT services provided by the GSA. EAC contracts separately for email, currently using a Microsoft Office 365 environment. EAC's website is hosted by a third-party provider.

Strategy | As a small agency, the EAC is attempting to reduce reliance on local servers and systems, opting for contracted services, primarily through the GSA. The EAC has developed an equipment replacement schedule for desktops and peripherals and is in the process of modernizing all equipment. EAC is working closely with DHS related to cybersecurity preparedness in elections and in evaluating EAC's own IT infrastructure. DHS reviewed all of EAC's systems in year 2017, and the EAC is contracting with an IT consultant to conduct a second review and make recommendations for execution by the new CIO. The EAC has adopted risk-mitigating approaches, particularly in the area of email, and does not host email servers.

Resources | The EAC is a small agency funded at less than $8 million in 2017. The EAC Executive Director strongly feels there is a need for greater emphasis on cybersecurity threats in elections.

Leadership | The EAC is working closely with GSA and DHS related to cybersecurity issues in elections. EAC employees—including the Director of Certification, Senior IT Specialist, and the Executive Director--will combine to work closely with GSA and IT consultants to manage EAC's IT infrastructure. The Executive Director has discussions with the IT staff daily, and is kept apprised of unusual hardware, software, or networking issues.

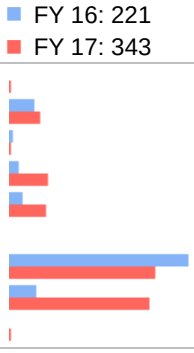
Inspector General Assessment

Although progress is needed to move to the next maturity level, EAC's overall information security program was effective based on the FY 2017 IG FISMA Reporting Metrics results and the related FY 2017 FISMA Audit. This audit included an evaluation of one information system at EAC. The audit noted 47 of the 60 selected NIST SP 800-53, Revision 4 security controls were properly implemented. The audit recommended that EAC enforce PIV Cards for local network authentication; maintain active interconnection agreements; maintain and review assessment and authorization packages; mitigate network vulnerabilities to strengthen controls over vulnerability management; strengthen controls surrounding audit logging and monitoring; improve procedures for third party contractor system oversight; update and test continuity plans; and strengthen management of Plans of Actions and Milestones.

FY 2017 Annual Cybersecurity Risk Management Assessment
Environmental Protection Agency

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	22	27
External/Removable Media	3	2
Improper Usage	9	34
Loss or Theft of Equipment	11	31
Physical Cause	NA	0
Web	153	126
Other	23	121
Multiple Attack Vectors	0	1



CIO Risk Management Self-Assessment

Risks | The Environmental Protection Agency (EPA) has determined that System-level risks, including those to HVAs supporting Mission Essential Functions, are at acceptable levels, though there are many unknown risks due to EPA's limited cybersecurity capabilities. This includes the ability to properly identify, engineer, and mitigate risks. As such, the agency's overall risk level is not acceptable.

Major risk areas include: insufficient resources to address risks; hardware and software asset management and authorization; vulnerability management; configuration management; identity and access management; insider threats; remote users; anti-phishing, malware, and exfiltration defenses; incident response; inadequate network capacity and architecture to support important security capabilities; legacy and emerging technologies; acquisitions processes, contracts, and contractor oversight; and sub-optimal staffing levels, skills, and organization. Furthermore, increased usage of mobile devices to meet mission needs could create additional risks.

Strategy | EPA's risk management strategic plan defines the agency's risk management strategy and how the agency frames, assesses, responds to, and monitors risk. Strategic risk, mission, systems and funding levels are all considerations taken into account when developing and implementing mitigation strategies, integrating both strategic and tactical goals. The risk management strategic plan also describes and regulates the agency's Enterprise Risk Management Process (ERMP), which is the mechanism by which EPA senior leaders and managers are formally informed of known risks. The ERMP integrates privacy, legal, mission, and public affairs considerations with cybersecurity risks. Once mature, the process will enable EPA senior leaders and managers to manage risk with an agency-wide perspective and to make consistent, informed risk-based decisions. The CISO monitors information security compliance, assesses control statuses, threats, and risks and makes recommendations to the CIO who serves as the agency's Risk Executive. The Risk Executive may take all necessary actions to reduce unacceptable risks to include shutting down systems, removing systems from, or isolating systems on, the EPA network and removing or limiting user access to systems.

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

EPA identified risk mitigation projects that are either new capabilities or significant changes to existing technologies or processes to close or mitigate known weaknesses. Congress appropriated $27 million to the risk mitigation projects in FY 2016, but additional funding is required. EPA estimates an additional $31.5 million in investments is needed in FY 2018 to address significant risks. EPA is also looking at multiple models for delivery of cyber services to control costs and improve capabilities. For example, EPA is exploring partnerships with other agencies to collaborate and leverage existing capabilities.

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

Inspector General Assessment

The EPA has an effective information security program. We concluded that the EPA fully defined its policies, procedures, and strategies to meet the requirements of the security functions and related domains outlined in the IG FISMA reporting metrics. The EPA asserted that it has fully implemented processes and activities consistent with the IG FISMA reporting metrics and provided artifacts and other documentation to support their assertions. Based on our analysis of this documentation and comparison of management's assertions against prior audit work, we concluded the evidence supported management's assertions,

and we determined that the agency's overall information security program was effective. We worked closely with EPA representatives and briefed them on each portion of the IG FISMA reporting metrics as the results were completed; collected management's feedback on our analysis; and, where appropriate, updated our analysis to incorporate management's feedback. We concluded that the EPA took sufficient steps to complete the requirements in order to reach Level 3 (Consistently Implemented) of the FISMA maturity model. Management agreed with our conclusions.

FY 2017 Annual Cybersecurity Risk Management Assessment

Equal Employment Opportunity Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	3	1
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	2	0
Other	14	3
Multiple Attack Vectors	1	0

CIO Risk Management Self-Assessment

Risks | The Equal Employment Opportunity Commission (EEOC) maintains a Cybersecurity Risk Register, which outlines ten enterprise-level cyber risks to EEOC mission essential functions. The agency's top three risks are:

- Improper securitization of Personally Identifiable Information causing increased risk of a data breach;
- Lack of implementation of two-factor authentication causing risk of unauthorized access to agency systems; and
- Potential for software applications to exceed end-of-life maintenance support.

Strategy | EEOC developed plans to mitigate the risks identified through its risk register process, including taking the following targeted actions:

- EEOC implemented encryption of data at rest for sensitive data submitted through its public portal and data loss protections for outgoing external email. In addition, EEOC will implement a secure storage area within SharePoint that enforces restricted access and data loss prevention technologies.
- EEOC is configuring Active Directory's identity service to support two-factor authentication using PIV cards. EEOC expects PIV two-factor authentication for non-privileged users during FY 2018.
- EEOC implemented compensating controls to reduce associated security risks with end-of-life platforms. This includes replacing legacy applications with cloud-based services, migrating content management systems and intranet to SharePoint, and replacing legacy software with newer technologies.

Resources | A major gap in mitigating EEOC's cyber risks has been its use of legacy systems. During FY 2017, EEOC is closing this technology gap by migrating to Active Directory Premium and Office 365. As a part of this migration, EEOC provided training and obtained consultant support to address workforce competency gaps introduced through the implementation of the new technology. EEOC is also updating policies and processes to take advantage of the new capabilities.

Leadership | In March 2017, EEOC's Acting Chair issued an ERM Policy Statement, requiring the implementation of effective risk management principles across all aspects of the EEOC. This statement designated a Chief Risk Officer, established an Executive Risk Steering Committee (ERSC), and documented EEOC's Risk Appetite. The following month, EEOC issued an ERM Policy Handbook, formalizing EEOC's ERM policies and practices.

Following the issuance of EEOC's ERM Policy Handbook, the Chief Risk Officer tasked the ERSC with conducting enterprise risk assessments, documenting risks into risk registers, and developing EEOC's initial risk profile. The ERSC presents prioritized risks to the Acting Chair for incorporation into EEOC's Enterprise Risk Profile. EEOC's Enterprise Risk Profile informs both the agency's comprehensive reform plan proposals and EEOC strategic priorities. At a minimum, the EEOC ERSC will meet quarterly, reporting to the agency's Chair.

Inspector General Assessment

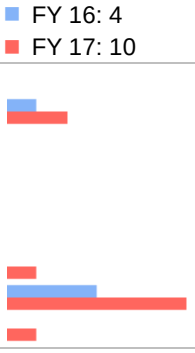
An independent assessor determined that the agency has an effective information security program. The independent assessor evaluated the EEOC's security control effectiveness with regard to whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies, utilizing the final FY 2017 Inspector General FISMA Metrics v1.0 maturity model. The overall assessment of EEOC's information system program is "Level 4: Managed and Measurable." EEOC's information system program could be improved by developing qualitative and quantitative performance measures and metrics in the areas of Detect, Respond, and Recover.

FY 2017 Annual Cybersecurity Risk Management Assessment

Export-Import Bank of the United States

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	2
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	1
Other	3	6
Multiple Attack Vectors	0	1



CIO Risk Management Self-Assessment

Risks | The Export-Import Bank of the United States' (EXIM) FY 2016 FISMA Audit identified the following high-priority areas of improvement:

- Low process maturity in applying the NIST Cybersecurity Framework;
- Skill gaps in EXIM's IT infrastructure operations and security domain staff;
- Delays in CDM implementation and lack of an updated deployment schedule;
- Inability to trace an event across multiple devices, which causes inefficiency in detecting the source and impact of an event; and
- Need for a well-funded capital replacement plan to maintain a secure infrastructure.

Strategy | EXIM developed and is implementing a plan to mature the Cybersecurity Function. EXIM is also continuing to mature its enterprise risk process, which will include at least three reviews per year of top enterprise risks. EXIM's risk mitigation approach is comprised of five tactics: 1) improving program maturity, 2) outsourcing and use of shared services for risk management, 3) simplifying and modernizing IT hardware assets, 4) fully staffing the cybersecurity and infrastructure operations function, 5) and improvement of the budget process to identify and account for cybersecurity costs.

Resources | EXIM's greatest challenge remains its workforce. Currently, EXIM does not have the hiring flexibilities to more successfully attract and retain key cybersecurity talent.

Additionally, EXIM has identified items within its IT/IT security budget request that are not fully funded. More funding would be needed to address EXIM's centralized log management risk, and future operations and maintenance costs of CDM have not yet been determined by DHS. As budget resources become available, EXIM will fund these initiatives on a prioritized basis. EXIM also requires budget stability and protection around core IT operating capabilities including cybersecurity.

Leadership | Senior leadership at EXIM is highly engaged in the ERM process. The CIO is a member of the Chairman's weekly senior staff meeting and provides updates on cybersecurity events and metrics to all senior staff. The Enterprise Risk Committee reviews a range of enterprise risks, including cybersecurity that EXIM is managing. The CIO is also a member of the Executive Working Committee, which governs and enacts cybersecurity policies and procedures. The CIO and senior bank leadership are also engaged in cybersecurity as part of the Continuity of Operations (COOP) process and frequently test management's ability to recover from loss of facilities and the interruption of key bank systems.

Inspector General Assessment

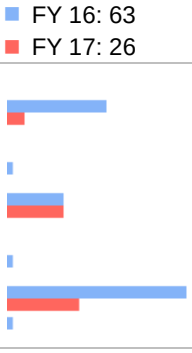
The OIG determined through independent review that the agency does not have an effective information security program. Based on the assessment performed, EXIM Bank is at an overall maturity level of Level 3, Consistently Implemented, an improvement over its prior rating of Level 2. While EXIM has made progress, key areas for improvement necessary to achieve Level 4 include revision of EXIM's vulnerability and configuration management processes; full implementation of its ERM program; improvement of its Information Security Continuous Monitoring and incident response programs by way of a dedicated Security Operations Center, a Security Incident and Event Management tool, and CDM implementation; and establishing qualitative and quantitative metrics to evaluate the effectiveness of each of the five Framework functions.

FY 2017 Annual Cybersecurity Risk Management Assessment

Farm Credit Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	18	3
External/Removable Media	0	0
Improper Usage	1	0
Loss or Theft of Equipment	10	10
Physical Cause	NA	0
Web	1	0
Other	32	13
Multiple Attack Vectors	1	0



CIO Risk Management Self-Assessment

Risks | Through its cybersecurity risk-management program, the Farm Credit Administration (FCA) is currently tracking over 36 risks. The five 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, including unauthorized network access.

Strategy | FCA selected Operationally Critical Threat, Asset, and Vulnerability Evaluation as a risk-management model. FCA documents the risk and develops a threat scenario, including how potential threat actors might exploit risk and who those potential threat actors are, determination of likelihood or probability, and how the asset's security requirements might be breached.

FCA's risk-management tool assigns risk scores according to likelihood, impact level, and the weighting of six impact-level categories. FCA develops a risk-mitigation strategy of compensating controls and assigns mitigation to responsible, supporting parties. FCA is upgrading its tools to also assign each mitigation an estimated budgetary resource requirement.

Resources | FCA continues to perform a detailed review of resource requirements for the agency; however, staffing is a primary concern. As a small, independent agency, FCA's Office of Information Technology (OIT) must perform the top-level compliance requirements of larger CFO Act agencies, while still providing the front-line, tactical support.

Leadership | The FCA risk register is reviewed by the CIO monthly. During these reviews, changes in risk factors are discussed and considered and management approves risks as final until reviewed again. The CIO discusses high-priority concerns with the Senior Staff Members and FCA Board Members, as appropriate.

Inspector General Assessment

An independent assessor determined that the agency has an effective information security program. The independent assessor performed the evaluation of FCA's security control effectiveness by assessing whether controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

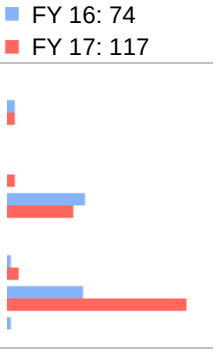
The evaluation uses the five NIST Cybersecurity Framework functions, broken into seven domains. The overall assessment of FCA's information system program is "Level 3: Consistently Implemented." FCA's information system program could improve by developing qualitative and quantitative performance measures and metrics in the areas of Detect, Respond, and Recover. The independent assessor made four recommendations to assist the FCA in strengthening its information security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Communications Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	3	3
External/Removable Media	0	0
Improper Usage	0	3
Loss or Theft of Equipment	34	29
Physical Cause	NA	0
Web	2	5
Other	33	77
Multiple Attack Vectors	2	0



CIO Risk Management Self-Assessment

Risks | The Federal Communications Commission (FCC) is focused on maturing its program to ensure effective management and reduction of cybersecurity risks. The agency is working to organize its capabilities around the NIST five function areas. FCC has recognized the risks to the agency, specifically those risks impacting its HVAs, including the Integrated Spectrum Auctions System (ISAS) and the Incentive Auction Bidding System (IABS) applications and infrastructure. The HVAs currently have open Plan of Action & Milestones. Risks to FCC mission essential functions (including the Disaster Information Reporting System) are not noted in the agency's internal assessments or audits.

FCC is committed to ensuring annual IT testing and disaster recovery capabilities are in place. Through FCC's internal assessments, FCC has over 850 open Plans of Action and Milestones for other systems (applications, database, operating systems), which need to be addressed. FCC is allocating resources to remediate these vulnerabilities based on the impact and severity.

Strategy | While the HVAs of FCC and mission essential functions are key focus areas, FCC has over 100 other IT systems. Consequently, to effectively manage risk holistically, FCC has established an ERM process. Through the ERM process, FCC will accept, mitigate, avoid, or transfer the risks that it discusses on a monthly basis. As risks are reviewed, the threat, likelihood, and impact are considered and an assessment of the risk's impact scope is made. FCC established risk criteria leveraging OMB Circular A-123 and the Chief Financial Officer Council Guide that drives the decisions made by senior management, including budgetary feasibility and prioritization based on criticality and impact.

Resources | FCC recognizes its critical cybersecurity gaps. While FCC is prioritizing application scans, over 30 critical control weaknesses related to denial of service, flaw remediation, and data input validation will require large development resources to be remediated. Based on vulnerability scans of the servers and critical databases, over 3,500 critical vulnerabilities still need to be patched. In addition, many legacy systems continue to run on an unsupported software/hardware or dated technology. Migrating from these dated technologies requires development and business resources.

Leadership | FCC is enhancing its monthly metrics to match those measured under the FISMA. These metrics have allowed FCC to further identify critical process improvements needed. These metrics are communicated to senior leadership.

Inspector General Assessment

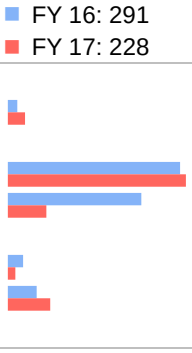
The FY 2017 FISMA evaluation included FCC's network (FCCNet), core financial management system (Genesis), Commission Registration System (CORES), and the Universal Service Administrative Company's (USAC) core financial management system (Great Plains). While FCC's information security program has improved since the FY 2016 FISMA evaluation in the areas of risk management, contractor oversight, and information security continuous monitoring, the independent assessor and the FCC OIG determined that FCC's overall program was ineffective in FY 2017. Specifically, OIG assessed FCC's security process related to the five NIST Cybersecurity Framework functions and determined that three functions were at maturity level 2, Defined, and two functions were at a maturity level 3, Consistently Implemented. Additionally, the independent assessor noted control weaknesses in each domain area within the five functions, with the exception of Security Training, which reached a maturity level of 4, Managed and Measurable. Going forward, the independent assessor recommends the FCC implement its documented security policies and procedures and establish ongoing monitoring over all five functions to achieve an effective maturity level 4, Managed and Measurable for its information security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Deposit Insurance Corporation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	8	14
External/Removable Media	0	0
Improper Usage	139	144
Loss or Theft of Equipment	108	31
Physical Cause	NA	0
Web	13	6
Other	23	33
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Federal Deposit Insurance Corporation's (FDIC) risks include: contingency planning, information security risk management, enterprise security architecture, governance, and technical obsolescence. Recent assessments of FDIC cybersecurity controls identified the following areas that require additional focus and resources to ensure greater cybersecurity across the agency:

- Alignment with NIST Cybersecurity Framework;
- Configuration baselines and configuration management;
- Critical file integrity monitoring;
- Enhance Chief Information Officer Organization (CIOO) Business Continuity Plans and Disaster Recovery Plans to include mission essential systems;
- Enhance management of privileged accounts;
- Enterprise risk management;
- Incident management and recovery;
- IT asset inventory management; and
- Network segmentation.

Strategy | The FDIC has integrated cybersecurity into its IT Strategic Plan and identified specific objectives addressing IT and cybersecurity risks. The FDIC is aligning its cybersecurity program with the NIST Cybersecurity Framework and is working closely with the Chief Risk Officer and other senior officials to manage corporate risks.

Based on the outcome of the agency's risk management process, the FDIC established corporate performance goals to reduce known or accepted risks and determined whether additional risk mitigation strategies should be implemented.

Resources | Decisions as to which investment to fund and the priority for each investment are based on internal control assessments, Government Accountability Office and OIG audit findings, or best practices that will lead to improvements across all risk domains.

In 2017, the FDIC received additional financial and human resources to execute solutions in-line with corporate goals and objectives as well as to address and mitigate known and unknown threats and vulnerabilities. The strategy communicated above ensures effective alignment of FDIC IT and security efforts and resources to address the most critical risks facing the corporation. The FDIC has added additional security resources and is actively working with DHS and commercial firms to discover and rapidly address critical risks.

During the 2018 budget formulation process, the FDIC will submit cybersecurity investments that will improve the FDIC's cybersecurity risk posture.

Leadership | Senior leadership is kept informed of cybersecurity risks on a continuous basis through in-person briefings, automated metrics and dashboards, and an annual assurance statement process.

FDIC senior leadership established the FDIC's IT Strategic Plan. The Plan integrates cybersecurity and sets corporate performance objectives with respect to cybersecurity. The CISO, on behalf of the CIO, and the Office of Corporate Risk Management (OCRM) established the Information Security Risk Advisory Council to provide a collaborative and integrated approach to the management of internal and external corporate risks that impact the FDIC's information security, elevate major internal and external risks to senior leadership, and prioritize those risks.

FDIC leadership is intimately involved in the funding and resourcing of IT and cybersecurity investments to address any identified gaps from the security and internal control assessment and external audit findings.

The FDIC has developed a customized ERM program for its mission, based on guidance in OMB Circular A-123. This program is supplemented with aspects of the Control Objectives for Information and Related Technologies framework within the CIO Organization. The constant interaction among FDIC senior leadership with OCRM and Corporate Management Control ensures the risk management output from the agency's ERM program along with other assessment activities, provides direct input into senior leadership decision-making processes for prioritizing the cybersecurity risk management activities.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. The assessment covered key components of FDIC's information security program and selected security controls pertaining to three general support systems, one application, and four outsourced service providers.

FDIC has established a number of controls and practices that were generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, FDIC had updated a number of its information security and privacy policy directives to align with government-

wide security policy and guidance and published an IT Strategic Plan that includes goals for strengthening information security and privacy.

However, FDIC's security program has areas of weaknesses that have limited the effectiveness of the program and placed the confidentiality, integrity, and availability of the Corporation's systems and data at risk. These include such areas as contingency planning, information security risk management, enterprise security architecture, and technology obsolescence.

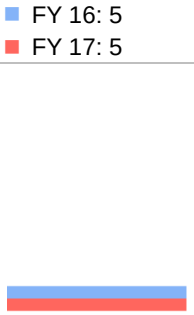
The assessment resulted in a series of recommendations to improve the effectiveness of FDIC's security program. FDIC is working to address all security weaknesses described in the report. A public Executive Summary of the assessment can be found at http://www.fdicig.gov/.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Energy Regulatory Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	5	5
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | To safeguard and protect its information and network, the Federal Energy Regulatory Commission (FERC, the Commission) employs a proactive cybersecurity program that incorporates the NIST RMF, Ongoing Authorization, and Continuous Monitoring. Since FERC faces energy industry-specific risks, it also leverages specialized intelligence sources to maintain awareness of current trends in potential adversaries.

To improve the Commission's ability to protect its HVAs, FERC conducts an annual Cybersecurity Program Maturity Model (CSPMM) review. The CSPMM is a critical on-site examination of the program to identify deficiencies, determine needed protections, and make recommendations. These have resulted in a strong cybersecurity program, with the Department of Energy IG identifying no findings over the last three years. FERC also procures external security assessment services on a biennial basis to provide reasonable assurance that adequate security controls are operating effectively.

Strategy | FERC's RMF program is an approach for transforming the three year Certification and Accreditation cycle to a risk-based process for monitoring information systems on a continuous basis. The RMF has enabled information system-related security risks to be managed consistent with FERC's mission and business objectives. In support of FERC's RMF program, the Commission has developed a tool based on NIST standards to assess security controls and determine the correlated risk associated with each control per system. FERC's RMF strategy also defines organizational roles across the enterprise.

Another key component of FERC's RMF strategy is the Vulnerability Management Plan, which outlines an approach for managing vulnerabilities and qualifying risks. This includes a waiver/deviation and tracking process for vulnerabilities that increase risk but cannot be mitigated due to environmental factors. This, along with the RMF and project-level risk logs, helps the Commission incorporate risk into business decisions.

Resources | FERC has a three year IT strategy in place to address gaps in capabilities and reduce risk. One goal is to reduce obsolete IT assets. To achieve this goal, FERC has incorporated projections of asset obsolescence into the Commission's budget requests, procurement decisions and modernization plans. FERC has also established review boards to avoid such technology gaps in the future. These forums provide executive oversight of IT programs and projects as well as a collaborative forum to discuss and fund FERC IT projects and their statuses.

In addition, FERC's aforementioned annual CSPMM reviews have identified gaps in the enterprise security posture including unsupported legacy systems and applications, reduced network visibility, and the need for modernization, all of which stemmed from a lack of prioritization and resources/funding. The CSPMM process has helped to justify the need to improve network visibility and modernize the network and, as a result, FERC is undergoing a network refresh, implementing new monitoring tools, and providing additional training for the Security Operations Team.

Leadership | Senior leadership plays an active role in the risk management process. FERC's CIO participates in the Commission's ERM process during which cybersecurity risk management strategy is integrated. The process members involved are FERC's senior leadership. Additionally, FERC has established a review board comprised of senior agency executives to ensure that all investments factor in risk while meeting the strategic and business objectives of FERC.

Senior executives are also briefed annually on FERC's IT Strategy, which defines objectives that aim to support the organization's strategic mission by providing secure, stable, and streamlined IT services that achieve cost and operational efficiencies. This strategy includes annual quantitative metrics, including a security risk rating that measures the efficacy of the security program. The risk rating provides senior management with cybersecurity risk awareness that enables them to make informed investment decisions that mitigate identified risks. It also supports and influences the agency's cybersecurity risk management strategy and ERM process.

Inspector General Assessment

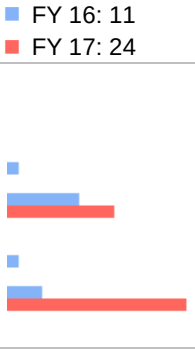
The OIG conducted the annual evaluation of the FERC's unclassified information security program to assess the effectiveness of unclassified information security policies, procedures, and practices within five information security functions (Identify, Protect, Detect, Respond, and Recover). The OIG determined that the Commission had an effective information security control environment. Specifically, the Commission had "Optimized" information security controls functions (Level 5) in Identify and Detect, "Managed and Measurable" information security control functions (Level 4) in Protect and Respond, and "Consistently Implemented" information security control functions (Level 3) in Recover.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Housing Finance Agency

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Optimized
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover	Managing Risk	Optimized

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	1	0
Loss or Theft of Equipment	6	9
Physical Cause	NA	0
Web	1	0
Other	3	15
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Federal Housing Finance Agency (FHFA) faces the same cybersecurity threats as other Federal agencies and organizations, including a recent increase in ransomware attacks.

Strategy | To address these risks, FHFA has implemented a defense-in-depth strategy that includes, but is not limited to:

- Blocking network communication to and from foreign countries;
- Implementing a layered perimeter security that includes DHS Einstein monitoring, web content filtering, intrusion prevention, email filtering, etc.;
- Implementing a next generation endpoint security solution to prevent zero-day attacks;
- Conducting network monitoring for anomalies and suspicious activity; and
- Conducting end-user security awareness training including phishing awareness simulations.

In the event of an attack, FHFA has implemented a robust data backup and recovery solution to allow the agency to restore data files with minimal impact on agency operations.

If an IT risk or control weakness is identified, members of the FHFA Security Team perform an initial assessment. If the risk can be remediated, it is either resolved immediately or documented and given a target completion date. This information is communicated to the Executive Committee on Internal Controls (ECIC) quarterly. Risks that cannot be resolved without adversely affecting FHFA's business operations are presented to management.

Resources | FHFA has identified a number of current gaps, most notable are infrequent compromise assessments and the lack of recovery plans related to public outreach and reputation management. Additionally, FHFA recognizes the need to deploy more granular access controls, and the agency is in the process of incorporating greater network segmentation. Finally, FHFA is awaiting software inventory technology through the CDM program, which it will not receive until FY 2018 Quarter 3.

Leadership | The agency's senior leadership determine its risk appetite and ensure the CIO, CISO, and supporting staff have the support and resources needed to implement an effective agency-wide cybersecurity program.

FHFA ECIC Risk Management Working Group establishes the ERM framework and provides recommendations to the FHFA Director. It also receives quarterly briefings from the CISO on emerging cybersecurity threats and metrics related to cybersecurity incidents, progress in meeting milestones, network vulnerabilities, and phishing simulation results.

Inspector General Assessment

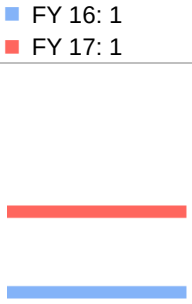
An independent public accounting firm (IPA) under contract and supervision of the Federal Housing Finance Agency (FHFA) OIG completed a performance audit to evaluate the effectiveness of FHFA's Information Security Program and practices and determined them to be effective. The IPA's methodology included testing the effectiveness of selected security controls implemented in FHFA's General Support System (GSS) and a subset of systems in accordance with the NIST's SP 800-53 Rev. 4. The IPA determined that FHFA's information security program complied with FISMA legislation and with OMB guidance, and that sampled security controls selected from NIST Special Publication 800-53, Rev. 4 demonstrated operating effectiveness.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Labor Relations Authority

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	1
Physical Cause	NA	0
Web	0	0
Other	1	0
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Federal Labor Relations Authority (FLRA) security program is resource-strapped and struggles at times to keep up with ever-changing security needs. Budget and personnel constraints represent the biggest threats to cybersecurity of the Authority. An absence of dedicated personnel whose sole responsibility is to attend to the Authority's cybersecurity program will undoubtedly increase the probability of an incident going unnoticed, software vulnerabilities not getting patched, or an insider threat going undetected.

Strategy | The FLRA attempts to strike a balance between risk management and user functionality and accessibility when determining how to handle risks. Simply 'managing risk' would often inconvenience the FLRA staff to a degree that would be considered untenable. For instance, since a large percentage of our user base is highly mobile, the FLRA has decided to enforce two-factor authentication only for access to functions that require elevated privilege.

If the FLRA were able to produce PIV cards for the staff (at headquarters and our six geographically diverse regional offices), the agency would be able to consider enabling two-factor authentication. Currently, it is cost prohibitive to purchase the necessary equipment and/or upgrade our service level with GSA to replace lost/stolen cards. As such, the FLRA continues to accept that risk.

Resources | Budget constraints currently prevent the Authority from putting PIV card printing machines in the seven geographic locations where the FLRA maintains a presence. The service level agreement we have with GSA does not allow us to provide the level of mobility that we need to provide the agency's users. For those reasons, it is likely that this gap will remain for the foreseeable future.

The FLRA also has a significant gap in information security personnel. There is currently no one solely dedicated to the information security program for the Authority. While the FLRA does attempt to leverage every human resource that it can to maintain the information security program, the authority's budget prevents employing a full-time information security professional, which is a risk that the FLRA has chosen to accept.

Leadership | The FLRA's small size allows for simplified and efficient communication channels. The IT staff meets weekly with the Executive Director to discuss any IT-related issues. The Executive Director meets weekly with the Authority's Chairman to convey concerns or other relevant information regarding IT and IT security. The Executive Director (and former CIO) is heavily engaged in information security decisions. All IT purchases (information security related and otherwise) over $3,000 are reviewed by the Executive Director before they can be approved by the Director of Budget and Finance. The senior leadership at the FLRA has a great deal of knowledge of the information security posture and program maintained by the Authority.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. There were no new issues. Of the prior year issues, only one was open, which involved the timely remediation of vulnerabilities.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Maritime Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	2
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	3	0
Other	0	1
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Federal Maritime Commission (FMC) has conducted an assessment of the risk of its information systems and has identified and accepted risks associated with not employing an automated incident handling reporting system.

The FMC has determined that technologies and connection types overall are at a moderate risk level, and that it does not operate any HVAs.

Strategy | FMC has fully implemented various tools to alert the CISO and network engineer in the event of anomalous behavior, privilege escalation, account creation or modification, unauthorized access, or failed access attempts. The FMC conducts regular network scans to identify and resolve network vulnerabilities, has implemented Managed Trusted Internet Protocol Service via a FedRAMP-certified provider, and is working with the DHS to deploy CDM program capabilities.

Resources | To comprehensively address and mitigate risks, the FMC has employed an array of investment strategies and IT tools to safeguard entrusted data, monitor for anomalous activity, conduct regular network scans, and ensure the most up-to-date training in cybersecurity and privacy. FMC has implemented Managed Trusted Internet Protocol Services, and as a FEDRAMP participant, is awaiting implementation of DHS CDM capabilities.

Leadership | The Commission's Information Technology Advisory Board (ITAB) functions as a technical resource to the agency and is the primary venue for the development and implementation of cybersecurity risk management strategy, support, and budget planning. The ITAB meets quarterly or as needed and keeps senior leadership apprised of the status of cybersecurity risk. The FMC also monitors user and file access activity and sends alerts to the Administrator and CISO.

Inspector General Assessment

The overall IG assessment rating is "effective" for the FY 2017 FISMA evaluation of the FMC. The assessment identified two weaknesses, and concluded the FMC had effectively implemented all prior year recommendations.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Mediation and Conciliation Service

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Federal Mediation and Conciliation Service (FMCS) does not host nor directly access any classified information systems. The principal risks to the agency are loss of information due to virus and malware attacks and loss of physical access to premises causing an inability to manage the environment. FMCS considers its risk level to be very low because the agency's Mission Essential Functions can continue to be performed without these systems for short periods of time. The agency has identified two sets of HVAs.

Strategy | FMCS's risk management approach utilizes three primary strategies:

- Transfer of risk to third parties for highly available systems (web servers, phone systems, and email);
- Mitigation of loss through near-real-time backup of internally hosted systems and data stores; and
- Prevention of system compromise through the use of enterprise level anti-virus and malware protection, configuration management and ongoing user education.

Resources | FMCS currently lacks full-time personnel dedicated to cybersecurity. The lack of resources reduces the agency's ability to implement the latest cybersecurity tools and processes. The solution that FMCS has identified is outsourcing these services to external organizations.

FMCS has also identified a gap in the capabilities of its data circuits. The agency is in the process of implementing TIC compliant data circuits through Managed Trusted Internet Protocol Services, which will allow the agency to utilize the Einstein E3A for continuous monitoring of network traffic.

Leadership | The agency states that its management is actively involved and has made the necessary budgetary commitments to implement the solutions it has identified. Additionally, it notes that senior management is briefed on a monthly basis.

Inspector General Assessment

An independent evaluation of the IT cybersecurity program for FMCS was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. The Federal Mediation and Conciliation Service will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Mine Safety and Health Review Commission

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	2
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Federal Mine Safety and Health Review Commission (FMSHRC) is working to develop a risk management strategy. As a micro-agency with less than 150 nodes and a small IT staff, FMSHRC has not formalized a risk management approach but plans to do so by December 31, 2017.

Strategy | IT strategy normally follows risk management best practices. FMSHRC is working to develop a feasible, risk-based approach.

Resources | FMSHRC has not yet identified resource gaps.

Leadership | Senior management is developing a formalized risk management approach and overall IT strategy.

Inspector General Assessment

An independent evaluation of the IT cybersecurity program for FMSHRC was not performed for FY 2017, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. The Federal Mine Safety and Health Review Commission will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Retirement Thrift Investment Board

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	1	15
Loss or Theft of Equipment	2	13
Physical Cause	NA	0
Web	0	1
Other	24	75
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | Overall, the security posture of the Federal Retirement Thrift Investment Board (FRTIB) needs significant strengthening as evidenced by the results of multiple audits and penetration tests. The agency has recently completed several accelerated projects to mitigate various risks associated with the enterprise including; system configurations, system design, legacy systems, defense-in-depth measures, and system assessments. The Chief Technology Officer prioritized the organization's objectives to reduce the current level of risk, focusing the agency's efforts on closing audit findings and integrating new technologies, procedures, and processes. The CISO continues to assess and closely monitor the security posture of the enterprise to support the essential functions of the agency and the overall improvement of the security posture.

Strategy | The agency formalized an ERM program that entails a top-down assessment of operational and strategic risks. The agency has performed a comprehensive Enterprise Risk Assessment in quarter one (Q1) FY 2018 and identified is developing a portfolio of internal and external risks that will be assessed annually. This assessment identified key risks in IT and serves as a key input in assisting FRTIB management to develop and implement risk treatment plans to address the deficiencies noted. In addition, this effort will assist in closing open audit findings.

Resources | The agency has allocated additional resources to design and implement remedial measures to address the gaps noted in the Enterprise Risk Assessment using a risk based prioritization approach.

Leadership | The ERM program has the full support of senior leadership and will ensure the agency's cybersecurity strategy is aligned to the agency's efforts to mitigate key risks. The Chief Technology Officer and the Chief Risk Officer collaborate and share pertinent risk information with other senior executives on a weekly basis via the Executive Leadership Council and other collaborative forums, which include other management levels within the organization. Risk and other security-related activities are also shared with the agency's Board members on a monthly basis.

Inspector General Assessment

The objective of the FY 2017 FISMA audit was to determine the effectiveness of FRTIB's information security program and practices across the seven FISMA domains. For each domain, an independent audit firm reviewed a combination of entity-wide and system-specific controls focused on four of FRTIB's information systems.

The audit found that, for FY 2017, FRTIB had not fully developed and implemented an effective, organization-wide information security program to identify, protect, detect, respond, and recover from information security weaknesses. Furthermore, the audit identified a number of control deficiencies related to people, process, and technology.

While FRTIB is in the process of addressing previously identified information security weaknesses, significant improvements are necessary to appropriately address FISMA requirements. As a result, the independent firm recommends that:

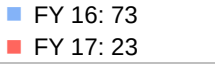
1) FRTIB clearly define an organization-wide risk-based information security program that is tailored to FRTIB's IT environment and information security risks; and
2) FRTIB reevaluate its existing governance structures to ensure appropriate oversight and monitoring over information security. In addition, FRTIB should assess the role that third parties play in regard to IT security, evaluate existing contractual agreements, clearly establish and define roles and responsibilities, and ensure that FRTIB has appropriate access to its information systems and data.

FY 2017 Annual Cybersecurity Risk Management Assessment

Federal Trade Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	25	6
External/Removable Media	0	0
Improper Usage	9	8
Loss or Theft of Equipment	1	0
Physical Cause	NA	0
Web	1	1
Other	34	6
Multiple Attack Vectors	3	2



CIO Risk Management Self-Assessment

Risks | The Federal Trade Commission (FTC) continues to make progress on implementing technical controls identified by OMB, meeting 75% of those metrics and closing all action items from its FY 2016 OMB CyberStat. The FTC also has made significant investments to close items identified by the OIG that affect the Commission's RMA rating. Currently, the FTC manages the risk of HVAs and Mission Essential Functions through a combination of cloud service providers and legacy IT at its on-premise data center. In some cases, the use of legacy IT increases organizational risk. For instance, due to resource limitations, the FTC cannot implement 24x7 coverage cost effectively.

The FTC accepts the risk regarding its aging legacy IT while it migrates to cloud services to improve network access control, consistent security configuration baselines, and network anomaly detection. As identified in the President's draft IT Modernization Report, the FTC will focus on the acquisition of emerging IT security models without solely relying on perimeter and signature-based defense.

Strategy | Starting in FY 2016, the FTC implemented an IT Strategy to reduce risks with legacy IT and contracts by prioritizing cloud-based shared services. Additionally, the agency aligned its risk management process with OMB Circular A-123 to mitigate implementation risks, including activities that address outstanding recommendations from the OIG.

Resources | The agency prioritized funding and recruitment of staff to address gaps identified through internal risk management and external assessments, such as the OIG's FISMA assessment and OMB's CyberStat. Concurrently, the agency restructured its approach to procurement practices to enable support of its IT Strategy. Lastly, the agency is planning to update its Cybersecurity workforce management plan to access key skills as competition for experienced cybersecurity professionals continues to increase.

Leadership | The Chairman engages with risk management leaders, including the Executive Director, CIO, CISO, and CPO on a regular basis. At an operational level, the Chairman has delegated IT risk management authority to the CIO. The CIO designates four individuals as Policy Management Authorities (PMAs) to manage decisions regarding identified issues and risks. Several Advisory Councils provide input on decisions as requested by PMAs. This approach enables timely and informed decision making by authorized staff. The CISO chairs the Cybersecurity Advisory Council, which includes all designated FTC Authorization Officials and System Owners.

PMAs log issues and risks in a repository available to senior leadership and advisory council members. In addition, PMAs and the CIO communicate issues and risks to senior agency boards established to support ERM. PMAs and responsible managers update milestones on a monthly basis, tracking progress against major risk management-related milestones. Those updates are reviewed with senior management via a quarterly PortfolioStat meeting and a monthly Senior Management Council meeting. The agency uses these meetings to drive prioritization of IT spending within FTC's budget and to balance the management of its information resources and risk effectively.

Inspector General Assessment

The OIG determined that the FTC currently provides effective protection for its information assets and that its information security and privacy programs comply with FISMA and related policies, standards, and guidelines of OMB, DHS, and NIST. However, the OIG also determined that the FTC's information security capability continues to be dependent on manual processes and legacy systems. FTC's information security program needs significant improvement if it is to continue to protect information assets and provide a mature information security control environment. The OIG assessed that FTC has weaknesses in each of the cybersecurity areas defined in the NIST Cybersecurity Framework. The OIG assessed that the FTC's information security program is at Level 3 (Consistently Implemented) for the Protect NIST Cybersecurity Framework function, and at Level 2 (Defined) for the remaining four functions: Identify, Detect, Respond, and Recover. The assessment showed that the maturity of the FTC information security program for the Identify and Respond functions decreased from Level 3 in FY 2016 to Level 2 in FY 2017. As the agency endeavors to modernize its IT environment in FY 2018, it needs to effectively and concurrently maintain legacy operations with managed change, risk-based decision-making, and effective continuous monitoring.

FY 2017 Annual Cybersecurity Risk Management Assessment

General Services Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	5	0
E-mail	174	78
External/Removable Media	0	0
Improper Usage	58	44
Loss or Theft of Equipment	335	230
Physical Cause	NA	0
Web	21	6
Other	72	76
Multiple Attack Vectors	0	1

CIO Risk Management Self-Assessment

Risks | The GSA is exposed to three primary risks: (1) the exploitation of sensitive information through email phishing attacks, (2) the lack of privileged, two-factor authentication, across all systems and devices, and (3) the lack of hardened security configurations across all systems and devices. While GSA is concerned with all of the risks cited above, the most substantial among them is exploitation through email phishing attacks. Additionally, while GSA has implemented two-factor authentication for all of its privileged network accounts, it is still working to implement for local system accounts. GSA is also working to further automate secure configurations across cloud systems in addition to those on-premises to ensure consistency and to allow for faster implementation.

Strategy | GSA's overall strategy for managing risk is a combination of acceptance and mitigation. The decision to mitigate or accept risk is made by the agency's Authorizing Official in consultation with its CISO. Generally, if a recognized risk cannot be reduced to an acceptable level, then the system, or component of the system, is taken off-line until the risk can be mitigated. Factors that go into these decisions include: active threat presence; likelihood of exploit; overall impact of successful exploit; and existence of other compensating controls. In addition to these risk factors, GSA considers strategic, operational, and budgetary factors and coordinates with program managers, the CFO, and the GSA Administrator. In some situations, risk cannot be mitigated completely. When these situations occur, GSA stakeholders meet to develop an interim plan to reduce risk to an acceptable level while GSA actively pursues complete risk mitigation.

Resources | GSA's identified resource gaps mostly relate to the prevention and/or reduction of the risk of phishing attacks. GSA currently uses a defense-in-depth strategy to mitigate this risk, which includes phishing training for employees and contractors. However, given that today's malware is often polymorphic and/or zero-day, more advanced defenses are required to mitigate and prevent attacks. GSA is actively pursuing next-generation AV software that uses artificial intelligence to stop malware of this advanced nature. However, despite improvements, current email malware technology within GSA does not completely stop malware from reaching end users' workstations. This gap represents a need for additional cutting-edge technology, such as virtual sandboxing, that can analyze malware before it reaches end users. Finally, GSA is working to close its enterprise-wide gaps in secure configuration of servers and adoption of two-factor privileged authentication, namely by coordinating with DHS to implement Phase 2 of the CDM Program.

Leadership | Over the course of the past year, the CIO and CISO regularly briefed the GSA Administrator, GSA Deputy Administrator, and other GSA Executives regarding the agency's cybersecurity status and risk management strategy. These briefings have consisted of the review of: quarterly PMC and FISMA performance metrics, which measure the agency's NIST Cybersecurity Framework implementation status; the prior Administration's Cybersecurity National Action Plan status and activities; and audit findings from GAO and OIG. During these briefings, recommendations have been offered and decisions made on cybersecurity issues, taking into account strategic, operational, budgetary, and security risk-based factors. Further, in accordance with OMB Circular A-123, GSA has established an ERM Program to track and monitor risks to the agency and its programs. Quarterly updates are provided through an agency risk register, which details all identified enterprise-level risks and enables the GSA ERM Group to equip leadership with risk information as it relates to agency strategic objectives.

Inspector General 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 5 NIST Cybersecurity Framework functions and 7 FISMA program areas. OIG identified 15 deficiencies within 3 of the 5 functions and 4 of the 7 FISMA metric domains. These deficiencies were identified in a selection of seven Federal and five contractor information systems.

Based on the maturity level that CyberScope calculates, it was determined that GSA's information security program was not effective because only one function was assessed at Managed and Measurable (Level 4), and the other four were assessed at the Consistently Implemented (Level 3), which is the current accepted requirement for effectiveness. We do note that GSA is currently in the process of implementing CDM Tools and Continuous Monitoring as a Service, ForeScout Agent Secure Connector, BigFix, Tenable, Splunk, and Archer.

FY 2017 Annual Cybersecurity Risk Management Assessment

Gulf Coast Ecosystem Restoration Council

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Gulf Coast Ecosystem Restoration Council (the Council) collaborates with other agencies to deliver IT infrastructure and IT capabilities to its employees. The Council relies on these Federal agencies to remain compliant with all FISMA and other cybersecurity directives, in addition to relying on their security teams to provide expertise. The Council ensures that endpoints are secure for accessing its assets within these partners' perimeters. The Council mitigates its risks by transferring them to entities that have expertise in ensuring IT assets are operating at a low risk.

Strategy | As a small agency, the Council's strategy is to partner with other Federal agencies and ensure the use of shared services. Collaborating with other agencies that have a full security staff is the best option due to its small size. This approach enables the agency to focus on endpoint protection.

Resources | The Council has identified gaps in ensuring Government furnished equipment endpoints are secure. In response, the Council is working with the DHS to implement the CDM program capabilities on its endpoints.

Leadership | The CIO is proactive in reviewing contracts to ensure they meet cybersecurity directives and keep senior staff up-to-date on IT issues. The CIO meets with the Deputy CFO on a weekly basis to ensure budget line items are included in the budget for IT security requirements and discuss IT risks. The DCFO then meets with the Director and Deputy Director to provide IT updates and any additional office administration updates.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. Consistent with applicable FISMA requirements; OMB policy and guidance; and the NIST's standards and guidelines; the Council's information security program and practices were established and are maintained for the five NIST Cybersecurity Framework functions and seven FISMA Metric Domains. However, for FY 2017, we identified one deficiency in the five functions and the seven FISMA Metric Domains. As a result, the maturity level of the program was given a score of "Defined." For the period of July 1, 2016 through June 30, 2017, the Council's information security program and practices were formalized and documented, but not consistently applied. As such, the Council's information security program and practices were not fully effective for the period of July 1, 2016 through June 30, 2017.

FY 2017 Annual Cybersecurity Risk Management Assessment

Institute of Museum and Library Services

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The results of the Institute of Museum and Library Services' (IMLS) risk assessment indicated that the agency had few critical vulnerabilities within its network. The assessment identified risks related to vulnerability areas of network isolation, managing removable media, patch management, and managing mobile devices.

Strategy | To address the identified vulnerabilities above, IMLS plans to develop actions related to the following: mitigating the network architecture risk by isolating internal network zones from the public-facing network; revising IMLS removal media detection and approval processes; ensuring network device patching timeliness is in accordance with the IMLS Patch Management Policy; and defining software installation privileges and logging.

Resources | IMLS is incorporating the above needs into resource requests which include ongoing enterprise migrations to the IMLS cloud computing environment, modernization of end user devices and software to address emerging gaps, and the replacement of the IMLS legacy grants management system with federal shared services.

Leadership | In preparing this report, the CIO reported to the Deputy Director of the Office of Digital and Information Strategy (ODIS). The CIO presented the materials associated with the strategy and regular OMB and DHS reporting to the IMLS Director (agency head).

Inspector General Assessment

IMLS not does not have an IG, but has periodically conducted independent assessments of their infrastructure. On July 7, 2017 the independent reviewer provided a Cybersecurity Risk Assessment and determined that the agency has an effective information security program. This assessment compared IMLS's process and practices to the five core functions (Identify, Protect, Detect, Respond, and Recover) of the NIST Cybersecurity Framework. The results indicate that IMLS has successfully implemented 73 percent of the Framework's subcategories and has an organization-wide approach to managing cybersecurity risk.

The independent reviewer recommends that IMLS implement several IT best practices and industry recommendations to mitigate the deficiencies identified during the risk assessment.

FY 2017 Annual Cybersecurity Risk Management Assessment
Inter-American Foundation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	1	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Inter-American Foundation (IAF) has identified numerous cybersecurity related risks, including the following:

1) IAF recently conducted a Security Assessment and Risk Assessment;
2) IAF does not have an alternate telecommunications agreement in place due to its small size and narrow mission;
3) IAF plans to implement a multi-factor authentication solution using PIV credentials by June 2018;
4) IAF has documented and tested the Incident Response Plan policy;
5) IAF plans to migrate HVAs to a cloud-based environment and test for disaster recovery in FY 2018;
6) IAF will be current on patching and Configuration Management on its HVAs in FY 2018.

Strategy | IAF plans to remediate all the above-mentioned risks except the need for configuring an alternate telecommunication service. IAF has chosen not to seek an alternate service, but the current IAF network is TIC compliant and utilizes a Managed Trusted Internet Protocol Services connection that offers redundancy.

Resources | IAF has not identified any resource gaps in its remediation of high-risk priorities.

Leadership | IAF has a strategy for organizational cybersecurity and risk management, including budget allocation, resource planning, and training. Senior leadership is frequently involved in the ongoing remediation of strategy and planning, including resource planning and budget allocation, by way of enterprise-level risk meetings, periodic audits, and approval of security policies.

Inspector General Assessment

IAF's information security program was evaluated based on alignment with the maturity metrics and as part of the FY 2017 FISMA Audit. The evaluation led to the determination of IAF having an overall effective information security program. The FY 2017 FISMA Audit noted that 86 of 94 selected NIST SP 800-53, Revision 4 security controls were properly implemented. The evaluation led to three recommendations for IAF, to improve its information security program:

1. Remediate unsupported software and configuration-related vulnerabilities in the network identified by the OIG, as appropriate, and document the results, or document acceptance of the risks of those vulnerabilities.
2. Document and implement a process to test system changes and document the results of testing.
3. Document and implement a process to test IAF's incident response capabilities.

FY 2017 Annual Cybersecurity Risk Management Assessment

International Boundary and Water Commission

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | Currently the cybersecurity risks at the International Boundary and Water Commission (IBWC) are moderate. Risk assessments conducted on GSS and SCADA Systems demonstrate the awareness and mitigation of existing risks to HVAs and Mission Essential Functions. A recent audit by the Department of State's OIG using metrics from the NIST Cybersecurity Framework showed no major concerns. Recent upgrades to the SCADA Systems has greatly improved IBWC's IT Security posture, and the implementation of additional controls are progressing. The agency's highest priorities are the lack of dual authentication capabilities, continuity of operations documentation and testing, training, and patch management of third party applications to mitigate existing vulnerabilities.

Strategy | IBWC's strategy for managing identified risks follows the established Plan of Action and Milestones process. At this time, the agency has not chosen to accept any existing risks or vulnerabilities identified during recent risk assessments. IBWC prioritizes risks and drives risk management decisions based on the likelihood and level of threat each risk represents to the environment. IBWC integrates budgetary considerations into decisions to mitigate risks, including reviews of all network devices and appliances to ensure the agency has considered their replacement costs and to mitigate known vulnerabilities within those devices. Continued costs related to IBWC's established services through DHS's CDM program are also considered in budget submissions. IBWC will be one of the first to obtain CDM services through the DHS developed blanket purchase agreement for CDM services, which will likely result in significant cost savings to the agency.

Resources | IBWC seeks to address its highest-priority risks, including patching and updating third party software within its IT environment. Although the agency has automated appliances and processes to patch and mitigate Windows-based patches, upgrading software and third -party applications (Java, Adobe) remains a manual process. IBWC is also leveraging existing full-time employees to address and mitigate high-priority application vulnerabilities on a regular basis, although this continues to be a challenge. IT staff is reviewing several additional patching and mitigation modules to include in the agency's existing solution to help address this gap.

Leadership | IBWC senior leadership plays a major role in the development and ongoing implementation of IBWC's cybersecurity risk management strategy. As a small agency, the IT department only needs to go through one staff layer to inform and request guidance on decisions related to cybersecurity risks. IBWC has processes in place to keep senior leadership apprised of risks within the enterprise, including weekly reports, quarterly Plan of Action and Milestones reviews, and frequent meetings directly with the CIO. The agency's CIO reports cybersecurity developments and information directly to the Commissioner during weekly staff meetings and immediately when necessary. The CIO is also the agency's Chief Accountability Officer, which allows for quick, informed decisions on how available resources are allocated to the IT cybersecurity program.

Inspector General Assessment

The OIG found that IBWC has generally implemented an effective information security program that supports the operations and assets of USIBWC. However, OIG noted multiple deficiencies that require remediation to fully comply with the FISMA Audit. Within the context of the maturity model, "Level 4: Managed and Measurable," represents an effective level of security. OIG concluded that three of the five domains assessed at IBWC—Risk Management, Configuration Management, Identify and Access Management, security training, and contingency planning—are performing at this level. However, OIG noted deficiencies that require remediation to fully comply with FISMA. OIG concluded that two of five domains—information security continuous monitoring and Incident Response—were performing at "Level 3: Consistently Implemented." OIG determined that these two domains and the configuration management metric (which is a component of the Configuration Management, Identify and Access Management, and security training domains) were performing at Level 3 because of issues related to the Supervisory Control and Data Acquisitions system at the South Bay International Wastewater Treatment Plant.

OIG made five recommendations in this report to address the deficiencies identified during the audit. In addition, four recommendations relating to previously reported findings in OIG's 2015 and 2016 FISMA audit reports remain open.

FY 2017 Annual Cybersecurity Risk Management Assessment
International Trade Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	3	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	3	0
Other	2	3
Multiple Attack Vectors	1	0

CIO Risk Management Self-Assessment

Risks | The International Trade Commission (ITC) determined that it does not currently possess any HVA, nor any Mission Essential Functions that cannot be deferred during an emergency or disaster. The ITC has identified the following risk categories currently being tracked and managed within the Commission's ERM program:

- System Authorizations: Some of the Commission's systems are lacking Authorizations to Operate.
- Data Centers: ITC headquarters' data center lacks redundant local loop communication circuits, but cannot be modernized without updates to the HVAC system. ITC also has hardware and software platforms that have reached their end of life.
- Recovery Planning: The Business Impact Analyses for the Commission's mission functions are in the nascent stage, with items impacting disaster recovery planning, contingency planning, and testing still unresolved. In addition, the ITC plans to move its headquarters data center out of its existing facility and into the co-located data center of one of its large Federal partners. Completion of ITC's data center migration and modernization efforts will support the agency's recovery planning efforts.

Strategy | Risks are identified and tracked at the office- level as a part of the ITC's Information Security Continuous Monitoring program, to include its CDM program, and its System Authorization program. When a risk is identified as an enterprise-level risk, it is entered into the ITC's ERM system. ITC leadership then evaluates the likelihood and impact of threats and vulnerabilities, weighing them against the ITC's strategic and operational priorities, as well as its budget, to determine risk prioritization. When risks impact a strategic goal or objective, the ITC's Performance Management Strategic Planning Commission (PMSPC) develops metrics that track performance of the strategic goal or objective against the risk.

The ITC has not accepted, avoided, or transferred any identified cybersecurity risks; instead, 11 cybersecurity risks are pending, seven are controlled, and five are closed.

Resources | The cost and availability of highly-skilled technical personnel is one of the ITC's highest-priority risks. The ITC leverages contractors to address many staffing needs; however, acquiring qualified and affordable contract personnel has proved challenging. The ITC is also unable to host TS-SCI clearances, which are necessary for senior cybersecurity staff to review classified threat feeds. ITC has also been unable to leverage many of the cybersecurity shared services its Federal partners like DHS provide.

Leadership | The ITC Cyber Security Division identifies and monitors cybersecurity risks, which are reported to the broader PMSPC. The PMSPC reports the metrics to Commission leadership at quarterly internal controls and risk management meetings. As needed, representatives from the PMSPC brief risks to the Commissioners and the Chairman at a monthly Commissioner's briefing.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. The ITC continues to focus on the important controls necessary to secure its network. These are composed of:

- Inventory of authorized and unauthorized devices;
- Inventory of authorized and unauthorized software;
- Secure configurations for hardware and software on mobile device laptops, workstations, and servers; and
- Continuous vulnerability assessment and remediation.

The Commission performs well for the most important security interventions, including agency-wide application whitelisting, 48-hour patching, and continuous inventory of network-connected devices. Additionally, the ITC improved its incident response management in FY 2017.

FY 2017 Annual Cybersecurity Risk Management Assessment

Japan-United States Friendship Commission

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Japan-United States Friendship Commission (JUSFC) does not handle classified information. Risks to the agency include the loss of availability and confidentiality, through data loss or disruptions to email communications.

Strategy | The JUSFC backs up data several times per day to mitigate the risk of loss.

Resources | The JUSFC is a small agency with four full-time employees. Protections are in place commensurate with the mission, size, and budget.

Leadership | All decisions regarding cybersecurity incorporate direction from JUSFC senior leadership.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for JUSFC was not performed for FY 2017 and the IG assessment section is marked “Not Applicable” (N/A). 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. JUSFC will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Marine Mammal Commission

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	At Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Marine Mammal Commission (MMC) has Microsoft Word processing, spreadsheet, and PDF documents that are created, maintained, and updated.

Strategy | To ensure documents are secure against threats, both natural and subversive, multiple backups are made and stored in several locations; including off line, off site, and fire proof containers.

Resources | This agency's gaps have been identified and planned for.

Leadership | All security plans and implementations are reviewed and approved by senior management on an on- going basis.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for MMC was not performed for FY 2017 and the IG assessment section is marked "Not Applicable" (N/A). 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. MMC will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Merit Systems Protection Board

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Defined
Protect	At Risk	Defined
Detect	At Risk	Defined
Respond	High Risk	Defined
Recover	High Risk	Defined

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	3
Loss or Theft of Equipment	0	2
Physical Cause	NA	0
Web	0	1
Other	3	2
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Merit Systems Protection Board's (MSPB) primary risk is its dependency on a singular data center. This data center is housed at the agency's headquarters office, which was not designed as a data center and presents challenges to optimal infrastructure care. MSPB also lacks a dedicated disaster recovery site. MSPB had not conducted a major security review in over three years, and contracted with the Department of Interior to perform an independent audit in August 2017. The DHS provides weekly vulnerability scans of MSPB's Internet-facing hosts.

Strategy | MSPB's Annual Performance Plan focuses on two primary goals. First, improving the stability and reliability of its IT environment. Second, modernizing its core business applications and migrating its data center to the cloud. MSPB is focused on adopting shared services to enhance its IT security posture. MSPB also set up an internal vulnerability scanner for its private network.

Resources | During FY 2015 and FY 2016, MSPB received independent reviews of its IT infrastructure. The resulting report identified staff competency gaps, including IT security.

Leadership | The Acting CIO/Senior Accountable Official for Risk Management reports to the Acting Chairman and Executive Director on a bi-weekly basis about risks within the enterprise.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. For FY 2017, MSPB is rated "Defined" in all six of the FISMA IG audit domains. MSPB does make a conscious effort to keep the network secure and comply with security standards and guidelines. MSPB has either defined or implemented several polices, or is in the process of creating policies and procedures, in an effort to meet FISMA and NIST standards. However, due to several factors, MSPB has not reached the FISMA levels of "Consistently Implemented" or "Managed and Measureable" throughout the FISMA audit domains. With the understanding that adequate human resources are a common issue for small agencies, immediate concerns and priorities include the following:

- The number of outdated or non-existent written policies and procedures;
- Procedures still in draft and not being fully executed;
- Lack of defined roles and responsibilities in terms of information security personnel; and
- Lack of automated processes to track security training, changes, and requirements.

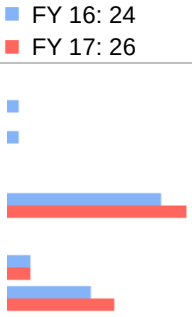
In FY 2018, MSPB will redouble its efforts and respond to these recommendations in order to improve its information security program as measured by the domain ratings. This includes obtaining an Authority to Operate for MSPB's General Support System (GSS) and using its Plan of Action and Milestones to systematically resolve identified deficiencies.

FY 2017 Annual Cybersecurity Risk Management Assessment

Millennium Challenge Corporation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	0
External/Removable Media	1	0
Improper Usage	0	0
Loss or Theft of Equipment	13	15
Physical Cause	NA	0
Web	2	2
Other	7	9
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | Millennium Challenge Corporation's (MCC) cybersecurity risks include:

- Lack of multi-factor authentication (MFA) across the enterprise;
- Weakening of the Enterprise's boundary protection through remote device connections allowing split tunneling from MCC's virtual private network to the Internet, and through personally-owned computers connecting to MCC's cloud email service;
- Personally-owned mobile devices connecting to MCC's cloud email service without a containerized solution; and
- Inability to sanitize or control the information processed through personally-owned computers.

Strategy | MCC is in the process of implementing an ERM program that includes an active oversight function, consistent with the requirements in OMB Circular A-123.

MCC has accepted the risk of split tunneling to overcome bandwidth constraints in remote overseas locations, most of which are located in developing countries with poor Internet connectivity.

MCC has also accepted the risk of allowing personally-owned computers to access cloud email services in order to enable performance for remote users; however, the agency plans to transition PODs to its mobile device management solution for containerized access. Furthermore, MCC plans to migrate to Windows 10 by FY 2018 Quarter 4 (Q4), which will remediate the risk of allowing PODs access to MCC's cloud email system. MCC will only allow domain computers to access this email solution after the transition.

Resources | MCC has identified the following gaps in its capabilities:

- Lack of multi-factor authentication across the agency, but it targets full compliance by March 31, 2018 and
- Lack of containerized solution to personally-owned mobile devices.

MCC has aligned budgets and resources to provide security capabilities. The assumed risks provide mission-critical access to information and resources.

Leadership | MCC's Executive Decision Group (EDG) includes the CEO, the Deputy CEO, and its five Vice Presidents, who convene to make agency decisions that are broad in scope and have significant impact. The EDG develops the agency's Risk Profile, reviews significant risks to the agency, determines appropriate risk responses, and assigns accountabilities for those responses. The EDG will review identified risks quarterly and will update the Risk Profile annually.

In addition, MCC has an Information Technology Investment Review Board (ITIRB), consisting of the five Vice Presidents and MCC's Chief Risk Officer. The ITIRB meets on a quarterly basis to review current and upcoming IT investments, and to identify risks and appropriate responses.

Inspector General Assessment

MCC's information security program audit included an evaluation of selected controls from three out of seven FISMA reportable systems at MCC. The audit noted 97 of 108 selected NIST Special Publication 800-53, Revision 4 security controls were properly implemented. This led to the determination of MCC having an overall effective information security program. There were a few recommendations made to help MCC improve their information security program. These recommendations can be found in the FY 2017 FISMA audit report.

FY 2017 Annual Cybersecurity Risk Management Assessment

Morris K. Udall Foundation

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	High Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Morris K. Udall Foundation's (the Foundation) lack of a TIC program is a priority risk. Due to a small IT budget, the implementation of Managed Trusted Internet Protocol Services was too costly for the agency.

Strategy | The Foundation currently uses cyber hygiene scans provided by the DHS to identify and respond to any vulnerabilities discovered. The agency responds immediately to high or critical vulnerabilities. The Federal Cyber Exposure Scorecard shows the agency as not having any active high or critical vulnerabilities.

Resources | The Foundation's largest gap is not having a TIC program. Efforts to establish a TIC program are delayed due to cost and hardware constraints. The Foundation is pursuing an independent assessment in order to classify systems and identify additional gaps. Costs, time, and personnel are the biggest challenges the Foundation faces as a small agency.

Leadership | In the past, the CFO functioned as the CIO. The agency has been without a CFO for six months and has just hired a new CFO who will ensure that cybersecurity is a priority.

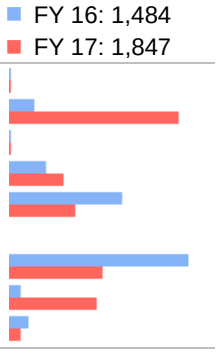
Inspector General Assessment

An independent evaluation of the IT cybersecurity program for the Foundation was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per the FISMA, Sec. 3555(b)(2), where agencies do not have an IG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. The Foundation will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment
National Aeronautics and Space Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	7	7
E-mail	99	646
External/Removable Media	11	3
Improper Usage	141	209
Loss or Theft of Equipment	427	249
Physical Cause	NA	0
Web	678	354
Other	44	333
Multiple Attack Vectors	77	46



CIO Risk Management Self-Assessment

Risks | The National Aeronautics and Space Administration (NASA) has improved its asset inventory management and security monitoring capabilities but requires attention in key areas. In particular, NASA plans to make improvements to its enterprise-level hardware and software inventory management capabilities; access management controls; exfiltration and network protection capabilities; and other processes that drive continuous improvement.

Strategy | NASA currently leverages a series of mechanisms to identify, manage, and mitigate agency cyber risk. NASA compiles periodic risk reports; conducts vulnerability scans and assessments with mitigation; and 24/7/365 Threat Monitoring and Incident Response.

While Corporate cyber risks are managed at the enterprise-level by OCIO and are understood, cyber risks to the Mission and Physical domains are less understood, with risk management and mitigation processes occurring within individual organizations. Going forward, NASA will manage cyber risk across the Corporate, Mission, and Physical layers in an integrated manner.

Resources | NASA assesses its quarterly performance in key Cross-agency Priority (CAP) areas in order to identify and align supporting budget, tools, people, and processes for priority gaps based on existing resources and the CIO's strategic goals. Specifically, the OCIO: (1) finalized its FY 2018 and FY 2019 security budget planning to fund key priorities, and (2) chartered the Cybersecurity Integration Team (CIT) to lead agency cybersecurity capability gap assessments and recommendations.

Recognizing cybersecurity's critical importance to NASA's mission and pursuant to implementing OMB's FY 2018 Capital Planning Guidance, NASA is restructuring its IT budget portfolio reporting – aligning IT Security investments across the agency with the NIST Cybersecurity Framework. The OCIO uses the Framework to organize its portfolio of security projects and budget to communicate and track resource use over time and promote better long-term resource planning.

Leadership | NASA leadership is implementing an ERM program across the agency, which includes cybersecurity as one of the top enterprise-level risks warranting agency attention. The Acting Administrator established the Enterprise Protection Program (EPP), which will protect strategic and critical capabilities and technologies from vulnerabilities (including cybersecurity).

To enable cooperative risk assessment, OCIO also chartered the CIT to implement the Framework across all three layers (Corporate, Mission, and Physical) and develop a cybersecurity risk management process that fully integrates into the broader ERM process. A significant challenge to cybersecurity risk management at NASA has been the historical lack of insight into cyber risk for NASA's Mission and Physical systems. The ERM process is expected to strengthen NASA senior leaders' insight and oversight of cyber risk.

Inspector General Assessment

For our FY 2017 review, we assessed NASA's information security policies, procedures, and practices by examining seven information systems. We also assessed the agency's overall cybersecurity posture using a variety of techniques and leveraged work performed by NASA and other oversight organizations. Finally, we evaluated the agency's progress in addressing deficiencies identified in prior FISMA and information security reviews. Collectively, those assessments assisted us in reaching our conclusions.

By implementing previous audit recommendations and taking additional corrective actions, NASA is steadily working to improve its overall information security posture. Nevertheless, as indicated by the results of this review, information security remains a significant challenge for NASA and the agency needs to take considerable action to close cybersecurity capability gaps and combat evolving cyber threats.

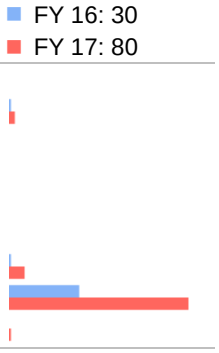
Although the agency continues to make progress in implementing cybersecurity initiatives, its cybersecurity program remains ineffective when judged using OMB's model, which requires agencies to achieve a maturity level of 4 (Managed and Measurable) to be considered effective. In the five function areas, NASA achieved maturity at Level 2 (Defined), indicating the agency's information systems remain vulnerable to serious security threats.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Archives and Records Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	2
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	1	6
Other	28	71
Multiple Attack Vectors	0	1



CIO Risk Management Self-Assessment

Risks | The National Archives and Records Administration (NARA) continues to improve its ability to protect the confidentiality, integrity, and availability of NARA resources. In FY 2016, the DHS performed a RVA and a Security Architecture Review of the agency's HVAs, resulting in the identification of weaknesses in NARA's HVA environment.

The NARA OIG also performed its annual security review and found that, while NARA made significant efforts to address weaknesses identified in previous evaluations and audits, improvement is still needed in seven of the eight FISMA metric domains. The OIG reported, however, that current programmatic initiatives, to include the funding of Information System Security Officer (ISSO) services, further improve NARA's information security program. These improvements will likely be realized starting in the next reporting period.

Strategy | NARA continuously monitors its environment to identify and assess risks in order to determine whether they should be accepted, transferred or mitigated. For this analysis, NARA considers risk factors such as the likelihood that a vulnerability will be exploited, and the impact to the agency in such an event. At a system level, vulnerabilities are managed and tracked. At the enterprise level, NARA tracks mitigation actions for programmatic weaknesses as part of its FISMA Improvement Plan.

In the event that a risk must be accepted, a formal request from the CIO to the NARA Chief Risk Officer is required. This evaluation considers several factors, such as the strategic, operational, and budgetary impacts the decision will have on the agency.

Resources | NARA has worked closely with DHS to identify and remediate weaknesses in the security architecture of its HVAs. This effort is a high priority for the agency, and resources have been dedicated to close identified gaps, and improve the security of these systems. This includes an integrated project team that meets regularly with DHS and is working to implement recommendations pursuant to the HVA evaluations. In addition to the team's work, NARA has funded additional resources, namely a dedicated ISSO and Security Engineer, to remediate residual weaknesses.

Furthermore, NARA Senior Executives have funded several other related efforts, to include:

- The acquisition of a commercial service bundle to improve monitoring, detection, response and recovery capabilities, as well as to extend coverage to 24/7;
- The acquisition of ISSO services to support System Owners in meeting their FISMA mandates;
- Funding the continuous implementation of HSPD-12 and Logical Access Control initiatives;
- Funding the continued support of three tools acquired through the DHS CDM Task Order 1 effort; and
- Funding the expansion of capabilities for existing security tools.

Leadership | Information concerning cybersecurity deficiencies, weakness, and risks is reported and briefed to the Management Controls Oversight Council (MCOC), the senior council responsible for overseeing the agency's internal control and risk management programs. The MCOC is co-chaired by the Chief of Management and Administration and the Chief Operating Officer, who also acts as NARA's Chief Risk Officer, as well as the Archivist of the United States and other Executives. The MCOC makes decisions on declaring a Material Weakness, and if a deficiency, weakness, or risk rises to such a level. Weakness status is provided to the MCOC on a quarterly basis to review progress and surface challenges to achieving projected goals.

Inspector General Assessment

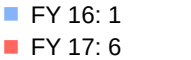
The OIG determined through independent review that the agency does not have an effective information security program. The OIG's assessment found NARA made improvements during FY 2017 throughout several domain areas: 1) NARA's Office of Information Services created the NIST Cybersecurity Framework Methodology (CFM) in order to record its repeatable policies and procedures.; 2) through the addition of ISSOs, NARA's development and maintenance of system security documentation generally improved; 3) NARA broadened its identification of risks by improving its RMF Dashboard to incorporate more systems; and 4) NARA's implementation of a scanning and monitoring service allowing 24/7 network monitoring capability. While we recognize these improvements, NARA will need to ensure it develops its capability to document, update, communicate, disseminate, and implement its program policies and procedures at both the organization and information system levels.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Capital Planning Commission

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	At Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	2
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	4
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The National Capital Planning Commission (NCPC) is responsible for protecting the confidentiality and integrity of proposed plans and projects throughout the review process until approved for public release. In this context, most data processed by the NCPC is public facing.

In terms of risks, the most common threats to NCPC information and information systems are user error during the performance of daily tasks, failures of equipment, environmental controls, and software aging. Adversarial threats, such as phishing emails, also pose a threat to NCPC's operating environment.

During the past several years, NCPC has focused efforts on improving cybersecurity; however, budget constraints have posed a serious challenge to these efforts. Any further cuts to the already meager IT security budget will have significant impacts to needed improvements. Where feasible, NCPC leverages cost-effective shared services to close security gaps, though these shared services are difficult to schedule.

Given its size, mission, and limited budgetary resources, NCPC was unable to acquire both IG services and robust IT tools and services to manage cybersecurity risks. NCPC made the risk-based decision to acquire essential tools and IT services to combat cybersecurity risks.

Strategy | Vulnerabilities identified in risk assessments are evaluated and prioritized by their impact to the agency's mission and business functions. Senior leaders make risk management decisions based on the overall impact to agency security.

NCPC accepts risks where mitigation efforts would inhibit mission operations or business functions. Senior leaders expect IT and security staff to implement compensating controls to the best extent possible to reduce potential impact and likelihood of exploitation. NCPC has a risk tolerant culture because its mission and business objectives do not affect the nation's critical infrastructure sector, nor do they result in the loss of Government continuity of operations.

Resources | NCPC leaders made a significant investment in modernizing infrastructure equipment and obtaining security engineering services to re-architect the network. NCPC staff is not well versed in incident detection and response. Instead the agency relies on the DHS' US-CERT for assistance in resolving incidents. NCPC hopes to alleviate this deficiency by participating in the CDM Program offered by DHS.

Leadership | Senior leaders play a critical role in the development and ongoing implementation of the NCPC cybersecurity risk management strategy. NCPC implemented a change management process that engages senior managers across the agency to review and approve proposed changes to the NCPC operating environment to ensure each division has input in enterprise architecture changes, including the acquisition of IT products and services. Changes that are processed through change management are reviewed by an advisory group, which is responsible for reviewing changes to determine its overall impact to enterprise operations.

The IT and security staff meet with senior leaders on a biweekly basis to communicate any project risks, issues, or concerns. NCPC senior leaders understand the importance of risk management and have made significant investments in the past years to make improvements for a more secure environment that does not hinder the agency mission or business operations.

Inspector General Assessment

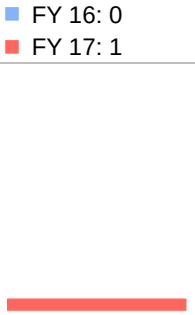
An independent evaluation of the status of the IT cybersecurity program for NCPC was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. National Capital Planning Commission will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Council on Disability

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	High Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	High Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	1
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | Federally-mandated cybersecurity requirements and the decentralized nature of the National Council on Disability's (NCD) IT infrastructure and systems make the agency's computing environment inherently difficult to manage and secure. Many subcomponents within the agency operate systems and applications needed to accommodate the disability community. In addition, the NCD has not developed or enforced standards or guidelines to reduce the risks commonly associated with heterogeneous computing environments.

Strategy | NCD's Information Security Office's (ISO) strategic objectives include a focus on data-loss prevention, improved security of system and network services, more proactive risk management, and incidence management.

NCD is undertaking initiatives that will assist the agency in reducing the likelihood of data loss and the resulting disclosure of confidential and Federally-protected data.

NCD initiatives focused on improving system and network security will support an in-depth defense architecture and provide increased security of critical NCD services. These initiatives and supporting projects are required through Federal regulations, including the FISMA.

NCD's risk management efforts will allow data owners and administrators to be more aware of information asset vulnerabilities. Administrators will then be able to identify controls to reduce those risks, and understand what risks remain after control implementation.

Incidence management initiatives are intended to assist NCD to recover its information assets in the event of a catastrophic event. Additionally, these initiatives will enable NCD to manage security events more effectively, thereby reducing or minimizing the damages to the NCD.

Leadership | NCD's Information Technology Security Specialist (ITSS), will lead the effort to deliver the agency's cybersecurity objectives. To be successful, the Information Security Office must align and coordinate resources with the various subcomponents across the agency.

Though NCD's cybersecurity governance process is still evolving, it anticipates that the stakeholders that participate in the decision-making process will include the aforementioned ITSS, under the management and direction of the Director of Operations. The ITSS is responsible for the overall management, direction, and security of NCD information systems, and is responsible for planning, developing, and deploying the NCD's Security Program. The Director of Operations is responsible for the evaluation and implementation of security initiatives, policies, and processes, while the Executive Committee is responsible for approving funds to support the oversight of security initiatives, policies, and processes. Finally, the Council is responsible for ensuring that the agency establish and maintain an information security program that protects NCD systems, services, and data against unauthorized use, disclosure, modification, damage, and loss.

Inspector General Assessment

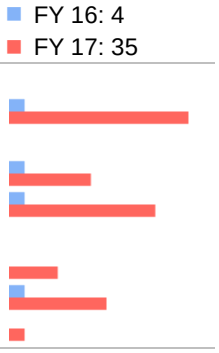
An independent evaluation of the status of the IT cybersecurity program for NCD was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. National Council on Disability will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Credit Union Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	11
External/Removable Media	0	0
Improper Usage	1	5
Loss or Theft of Equipment	1	9
Physical Cause	NA	0
Web	0	3
Other	1	6
Multiple Attack Vectors	0	1



CIO Risk Management Self-Assessment

- Risks | The National Credit Union Administration (NCUA) conducted assessments of its information security program in January 2016 utilizing the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool and the NIST's Baldrige Cybersecurity Excellence Builder. The program is currently assessed at Level II, while the agency notes the following key risk areas: Logical Access for State Examiners: NCUA is unable to enforce Homeland Security Presidential Directive 12 (HSPD-12) and Identity Credential and Access Management requirements with its State partners, but is finalizing implementation of a secure Business Partner Gateway with a compensating multi-factor authentication and authorization;
- Data Management Security: The absence of an Enterprise Data Reference Model (DRM) has resulted in weak protections for data holdings. The agency continues to conduct an exhaustive inventory of all data to ensure protections are in place;
- Legacy Application Security: NCUA is conducting binary and static code analysis to identify vulnerabilities and assess the feasibility of repairs or compensating controls for legacy systems;
- USB/Whitelisting for NCUA Examiners: Many Credit Unions desire the use of their own thumb drives on their networks during assessments, but this poses a risk of exposure to malware or insider threats. NCUA is implementing USB restrictions on all agency assets and will require credit unions to utilize one of its approved, secure data transfer mechanisms in the first quarter of 2018; and
- HVAs: NCUA has validated its HVAs in line with a Business Process Analysis (BPA) and Business Impact Assessment (BIA) with an emphasis on Mission Essential Functions and Essential Supporting Activities (ESA). NCUA is now normalizing the alerting capabilities for the HVAs to be further tested in its next table top exercises.

Strategy | NCUA has designated a low-risk appetite for IT with the exception of "Innovation," which has been designated as moderate. Based on these designations, the agency does not accept risk unless the weakness cannot be mitigated within the influence of the agency.

NCUA plans to achieve Maturity Level III in calendar year 2018 and Level IV in CY 2019 with risk acceptance where required. To minimize exposure while maturing the program, the agency has adopted the NIST Critical Security Controls (CSC) as Core Controls, to be assessed annually for all systems regardless of maturity level.

Resources | While NCUA believes it is staffed, budgeted, and has resources to support its priority and ongoing cybersecurity responsibilities, two areas of concern are presented:

(1) As cited in the risk identification, NCUA is unable to consistently get state partner's to adhere to HSPD-12 requirements for credentialing. Each State has a different set of suitability and background investigation practices as well as a lack of adoption of PIV-I approved by NIST. This requires the Federal government at large to collaborate as to how states and tribes will adhere to the HSPD-12 and FICAM requirements when conducting business with the federal government as a federated partner; and

(2) The gap presented by Digital Rights Management requirement of the Cybersecurity Act of 2015 is one of maturity and sequencing. NCUA continues to explore methods for adopting this capability as it continues with Data Management; Legacy Application; and overall Identity, Credential, and Access Management challenges, as they are prerequisites to a successful implementation of DRM.

Leadership | The NCUA established the Enterprise Risk Management Committee to address the ERM process as required by the OMB Circular A-123. Facilitated by the CFO and consisting of the executive leadership, this committee meets quarterly. The Cyber Security Steering Committee, facilitated by the CIO and the CISO, consisting of executive leadership, addresses risk and threats specific to the agency's information security program focus areas and meets monthly. The results of both committee meetings are presented to the Chairman and Board members accordingly, and has resulted in cybersecurity being a prominent aspect of the agency's strategy plan.

Inspector General Assessment

The NCUA OIG conducted an independent evaluation of the NCUA information security program for FY 2017 for compliance with the FISMA and federal regulations and standards. The OIG assessed the OCIO on all Function areas and underlying Domains identified in the FY 2017 IG FISMA reporting metrics. The OIG determined the NCUA has continued to strengthen its information security program and has an effective information security program.

Specifically, the OIG determined the NCUA: has addressed and resolved the remaining two open recommendations from FY 2015 FISMA; has addressed and resolved 17 of the 23 recommendations from FY 2016 FISMA on or ahead of schedule; and is in the process of addressing and resolving the remaining

six FY 2016 FISMA recommendations that the NCUA OCIO indicated - in response to the FY 2016 FISMA OIG review - it would resolve on completion dates after the end of FY 2017 FISMA. In this year's FISMA review, the OIG identified areas for improvement in risk management, identify and access management, information security continuous monitoring, and security training. The OIG made eight recommendations, which should help the NCUA OCIO continue to improve the effectiveness of its information security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Endowment for the Arts

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	1	0
Other	0	1
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The National Endowment for the Arts (NEA) established its ERM function in 2017 to identify, assess, and manage its mission-critical risks while continually improving governance, increasing accountability, and enhancing overall performance. The NEA does not have any systems identified as HVAs. Under Executive Order 13587, the insider threat program is for classified environments, of which NEA does not have any; however, NEA proactively developed an insider threat program and provided insider threat awareness training to its staff.

Strategy | The NEA has a Risk Management Council (oversight and management body) that includes representation from both the business and IT staff. The Council is responsible for decisions to accept, transfer, or mitigate risk. This includes defining objectives in specific and measurable terms that enable management to identify, analyze, and respond to risks related to achieving those objectives.

Resources | NEA conducted a risk assessment on the enhanced use of cloud capabilities. Continuous improvement is being made regarding data recovery using limited resources and leveraging Federal employees.

Leadership | NEA employs a RMF to routinely evaluate program areas and strategic initiatives. This evaluation balances risk with constrained resources, funding within the programs, and other operational needs. The NEA RMF establishes a consistent process whereby it identifies and prioritizes risks and strategies to address those risks. Lastly, at the end of FY 2017, the NEA hired a new CIO and appointed a new CISO.

Inspector General Assessment

As required by the FISMA, the OIG conducted an audit of the effectiveness of the NEA information security program for FY 2017. The audit was conducted in compliance with the guidelines established by the OMB in the FY 2017 IG FISMA Reporting Metrics and assessed the effectiveness of the following FISMA metric domains: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning.

The assessment found that the NEA has made partial improvements to the information security program; however, overall it was determined that the NEA does not have an effective organization-wide information security program. Specifically, the NEA did not fully develop an organization-wide information security risk management strategy to identify, assess, respond to, and monitor information security risk at all levels of the organization; nor did it fully develop information security program policies and procedures to guide the information security program.

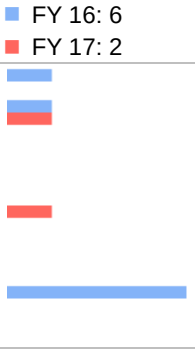
Recommendations include further developing an information security risk management strategy in accordance with NIST standards; updating all information security program policies; developing all applicable information security program procedures; and implementing stronger controls over privileged user accounts.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Endowment for the Humanities

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	1	0
E-mail	1	1
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	1
Physical Cause	NA	0
Web	0	0
Other	4	0
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The National Endowment for the Humanities' (NEH) major cybersecurity risks are mostly related to lack of funds and staffing. Specifically, the agency has identified several risks:

- Some systems have trouble utilizing two-factor authentication.
- The main NEH website is currently running an unsupported web content manager, which means it no longer receives regular security patches.
- NEH has not yet implemented DNSSEC.
- Several of NEH's system assessments and authorizations are out of date.
- CDM is not fully in place yet.
- The agency does not have a dedicated cybersecurity staff member.

Strategy | NEH has adopted the following steps and strategies for mitigating the identified risks:

- Upgrade to an active directory system that enables location-based two-factor authentication, while limiting remote email access, particularly with staff members that deal with PII.
- Hire dedicated cybersecurity staff member to improve responsiveness to security threats and maintain baseline controls. This includes performing A&As.
- Deploy existing CDM tools while seeking to implement the full suite of CDM tools. NEH is working with DHS; NEH is part of TO2F grouping.

In FY 2017, NEH signed a contract for DNSSEC capabilities and began redeveloping the agency's website to the current version of Drupal. Both of these tasks are expected to be completed in FY 2018.

Resources | NEH's biggest gap is funding for cybersecurity activities. The agency's small administrative budget makes it difficult to put in place the kind of robust cybersecurity program found in larger agencies. NEH is forced to share cybersecurity responsibilities across a small IT staff that does everything from workstation installations to helpdesk to security training. Budget is also a driver for other cybersecurity risks, which currently restricts in-house A&As or deploying a supported web server.

Leadership | The CIO meets monthly with the agency's Deputy Chairman and Assistant Chairman for Operations. During these meetings, the CIO briefs senior leadership on IT-related matters, including cybersecurity. For example, the CIO recently had a series of meetings with Senior Management and raised the aforementioned website issue, for which remediation efforts have begun.

Inspector General Assessment

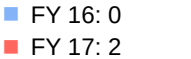
The OIG determined through independent review that the agency does not have an effective information security program. The NEH information security program has been designed consistent with NIST and FISMA requirements. However, the size of the agency and budgetary constraints have presented challenges in the agency ability to fully implement core elements of Information Security Continuous Monitoring and contingency planning, which impact the overall effectiveness of the program.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Labor Relations Board

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	1
Other	0	0
Multiple Attack Vectors	0	1



CIO Risk Management Self-Assessment

Risks | Internal cybersecurity reviews of National Labor Relations Board (NLRB) systems (including HVAs) identified that unsupported legacy and borderline legacy systems, social engineering, and deferred cybersecurity investments represent the most serious cybersecurity risks at the agency.

Two of the agency's three major applications supporting Mission Essential Functions have subsystems running on an unsupported operating system and applications that are nearing the end of support, which introduce security vulnerabilities and risky platform dependencies. These older technologies also hinder migration plans to cloud-based platform and software solutions.

In addition to concerns around legacy systems, the NLRB failed to meet performance targets in the DHS' Anti-Phishing Campaign Assessment this FY, indicating a need for more intensive training and better phishing mitigation technologies.

Across the agency, NLRB has accepted smaller risks due to resource constraints, delayed implementation of shared solutions, and expensive compliance directives. These smaller risks include the lack of outbound traffic decryption and inspection, which would double the cost of firewall upgrades. In addition, delays in the DHS's CDM task order have postponed the upgrade of foundational cyber tools. Finally, the Managed Trusted Internet Protocol Services program mandates greatly increased internet connectivity costs while forcing deferment of other cybersecurity investments, such as automated security event and information management tools. The aggregated risks associated with these deferred investments degrade the effectiveness of the cybersecurity program in important ways. Budget constraints and compliance mandates can distort risk management decision making in ways that cannot always be analyzed contemporaneously.

While all agencies are charged with protecting their IT systems regardless of resource constraints, the real-world impact of some risk trade-offs can be exacerbated for small agencies.

Strategy | NLRB's risk management approach currently relies primarily on our implementation of the NIST RMF, particularly the Plan of Action and Milestones process. Since 2014, a strategy has been in place for implementing Information Security Continuous Monitoring that incorporates the three-tiered organizational risk management approach outlined in NIST SP 800-39. The Information Security Continuous Monitoring strategy aims to achieve risk-based ongoing authorizations using automated tools from the CDM program. Currently, decisions to accept, transfer, or mitigate risk are made using the Plan of Action and Milestones process and as part of the system assessment and authorization process. The Information Security Continuous Monitoring strategy has dependencies on the CDM task order for the small agencies, and due to the task order delays, it is only partially implemented.

Resources | Addressing NLRB's legacy IT systems would require reengineering two mission systems. The agency uses contractors to develop, implement, and maintain these systems. Based on previous contracts, the agency estimates the updates to result in a serious budgetary burden.

The agency must enhance its current cybersecurity awareness training, which it can do using expertise from DHS, but could also require the acquisition of a phishing campaign management and assessment tool.

The smaller risks can be addressed through more aggressive cybersecurity governance at NLRB, at Federal shared service providers, and other oversight agencies.

Leadership | Senior agency leadership, including the agency head, review the risk management strategy process annually in connection with the FISMA audit submissions and results. Senior agency leaders have defined roles and engagement frequencies in the draft implementation of OMB Circular A-123, which will be implemented in FY 2018.

Inspector General Assessment

Our assessment scope was FY 2017. For that period of time, we determined that the NLRB did not have the policies and procedures in place that would generally meet the NIST requirements and was rated as not effective. Our assessment is consistent with findings that were developed during the FY 2017 financial statements audit. During FY 2018, we will review the steps taken by the NLRB to implement the recommendations that are intended to remediate the noted deficiencies by establishing and implementing documented policies and procedures that meet the NIST Special Publication 800-53 requirements.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Mediation Board

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The National Mediation Board (NMB) identified the following risks:

- The agency's public facing website needs to be converted to HTTPS, as do two in house service applications;
- agency users can access risky web applications;
- Insufficient device management and configuration; and
- Lack of agency controls around remote login to Department of Treasury and Department of the Interior applications.

Strategy | The NMB started projects to update its website and service applications this year. NMB also automated real-time configuration management and policies, and reviews these configurations weekly. The agency bans all new applications and requires manual approval prior to their deployment.

Resources | The agency must develop processes to approve procuring and deploying devices and applications by agency security staff.

Leadership | Risk assessments and cybersecurity plan changes are submitted to the Chief of Staff. There is a quarterly review of cybersecurity and Plans of Action and Milestones.

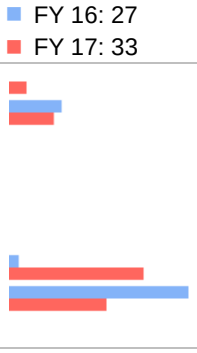
Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for NMB was not performed for FY 2017, 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. National Mediation Board will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment
National Science Foundation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	2
E-mail	6	5
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	1	15
Other	20	11
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The National Science Foundation's (NSF) top cybersecurity concern is to reduce the risk of data loss from Advanced Persistent Threats, particularly under the NIST Cybersecurity Framework Detect functions. Phishing, insider threats, unauthorized access to sensitive data, and zero-day threats are also significant concerns.

NSF addresses its risks through established layers of security controls to ensure its most significant information systems and assets are protected. These layers of controls include technical and operational controls, preventive controls, and detection and recovery controls. Through NSF's Information Security Continuous Monitoring program, NSF assesses the security state of information systems based on the FISMA security requirements and the NIST Cybersecurity Framework.

NSF leverages the services of the DHS to conduct weekly Cyber Hygiene Assessments of the external network and periodic RVAs. NSF uses DHS's CDM program's products to provide continuous monitoring tools and services to further assess its IT Security Program.

Strategy | NSF established a layered approach to IT security. Management controls include security awareness training and an Insider Threat Program. Use of PIV two-factor authentication for both privileged and unprivileged users is a key security control, and NSF recently implemented CDM and other tools for comprehensive management of privileged user access and access tracking. NSF is also in the process of implementing application whitelisting and has technical controls to monitor the network and provide malware and intrusion detection. NSF is also enhancing email and web traffic filtering products to protect against external threats.

When attacks do occur, NSF takes steps to contain, eradicate, and recover from the attack. NSF also installed a monitoring tool designed to protect against zero-day threats, reviewed and modified incident handling procedures, expanded procedures on phishing, modified training, and strengthened processes to more effectively identify and safeguard against future attacks.

NSF invests in robust solutions to meet serious and evolving cyber threats. NSF continues to invest in IT security projects.

Resources | NSF has not identified significant gaps in its ability to resolve its highest-priority risks and continues to pursue government-wide targets for software asset management and malware defense.

NSF is implementing multiple solutions, including application whitelisting, to address the risk posed by malware. NSF is also implementing near real-time monitoring of web and email traffic. CDM Phase 1 will provide tools to allow only authorized software to be installed on NSF devices, and Phase 2 will improve access controls and modernize security tools. NSF is also implementing Data Loss Prevention software to reduce the threat of a major PII breach. Software to detect the attempted exfiltration of sensitive information is being tested and planned for deployment in FY 2018.

NSF has aligned resources to provide the capabilities needed to close gaps and is working toward full alignment with the NIST Cybersecurity Framework to manage and reduce cybersecurity risk.

NSF benefits from shared services, utilizing the capabilities of a Trusted Internet Connection-compliant provider for routing agency network traffic as well as the Federally-provided intrusion detection system. The DHS Cyber Hygiene and RVA provides specific risk analysis support.

Leadership | The CIO briefs NSF senior executive management, including the NSF Director, Deputy Director, and the National Science Board, on topics and issues related to IT and cybersecurity as needed. The CISO, on behalf of the CIO, develops and maintains the NSF IT Security Program, including ensuring compliance with legislation, government policy, and guidance. The CISO is also responsible for performing risk management activities and assessments in compliance with applicable requirements.

The CIO chairs the Executive Information Technology Resources Board (ITRB), which manages the NSF IT investment portfolio and enterprise architecture, providing governance and executive-level oversight of IT plans to ensure the investment portfolio aligns with NSF mission goals and priorities. The Executive ITRB also approves NSF's IT investments and IT budget requests, assesses alignment of IT investments with NSF strategic goals, and monitors performance of IT investments.

Inspector General Assessment

In order to assess how the National Science Foundation (NSF) established its agency-wide Information Security Program and practices, as required by FISMA, an independent assessor performed detailed testing of NSF's iTRAK Application and the systems and applications supporting the United States Antarctic Program (USAP) for compliance with selected NIST SP 800-53,

Revision (Rev.) 4 controls. Overall, the Information Security Program was rated positively and as effective; however, continued management attention is necessary in the Protect – Configuration Management function. For this function, the independent assessor identified that NSF scored below the "consistently implemented" level in one of eight security metrics within that function.

FY 2017 Annual Cybersecurity Risk Management Assessment

National Transportation Safety Board

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	2	1
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | As part of the National Transportation Safety Board's (NTSB) ongoing internal assessments, third-party assessments, and annual IG reviews, the NTSB is currently tracking and addressing nine major risks to its cybersecurity posture. These risks are focused in the areas of logical PIV card authentication, privacy program reviews and updates, Domain Name Systems Security Extensions, and implementing Internet Protocol Version 6 (IPV6) on public facing systems.

Strategy | The NTSB has implemented a Plan of Action and Milestones tracking process in which CIO managers meet biweekly to review progress toward open items and send a monthly report to the agency head.

Resources | NTSB faces a significant gap in logical PIV card deployments. Agency management responded to this need by authorizing additional staffing resources to close the skills gap. NTSB also leveraged the DHS' CDM program offerings to assist with both the skills and budgeting challenges to meet this mandate.

Leadership | Senior leadership is briefed monthly by the CIO to discuss open risks and challenges to closing them out. As a result of these meetings, necessary resources, funding, or risk acceptance is discussed and evaluated to align with the NTSB mission, risk posture, and requirements.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. Upon completion of the audit it is apparent that the NTSB has gone through extensive efforts in securing the organization's GSS environment and has complied with most security control requirements tested during the security assessment of the NTSB information security program and NTSB information systems. The NTSB information security program was found to be implemented effectively due to factors validated by operational evidence.

FY 2017 Annual Cybersecurity Risk Management Assessment

Nuclear Regulatory Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	1	3
External/Removable Media	0	0
Improper Usage	7	12
Loss or Theft of Equipment	2	1
Physical Cause	NA	0
Web	0	0
Other	14	23
Multiple Attack Vectors	1	1

CIO Risk Management Self-Assessment

Risks | The NRC utilizes a defense in-depth strategy for cybersecurity infrastructure, whereby additional controls are placed upon information that is critical to the agency's Mission Essential Functions and HVAs.

The NRC conducts external penetration tests annually to ensure that perimeter defenses are effective against a variety of technical and social engineering attacks. The NRC also uses NSA's Information Assurance Directorate and DHS resources to conduct internal and HVA assessments on a recurring basis. DHS has conducted two assessments of NRC's HVAs in the past year -- one a technical assessment, the other an architectural review. Both assessments determined that while NRC was utilizing appropriate security controls, there were opportunities to improve the NRC's resilience against cyber-threats.

Additionally, the NRC's IG, GSA, and OMB each provide/review assessments conducted by other entities to ensure that the NRC addresses the findings from each assessment. The NRC has also implemented CDM tools to increase its security posture and prioritize findings based upon the sensitivity of data contained within each boundary. As a result, there are no remaining open critical or high vulnerabilities from any of these assessments.

Strategy | The NRC developed and uses a Cybersecurity Risk Dashboard (CRDB) to measure its progress on continuous monitoring, training, and FISMA compliance efforts. The CRDB quantifies the cybersecurity risk posture of the agency, increases awareness of cybersecurity risks, tracks cybersecurity at the office level, and provides information critical to prioritizing cybersecurity and other IT investments for budgeting and planning purposes.

Another avenue for managing risk is the NRC's Change Control Board (CCB). The CCB reviews the operational risk of system changes and conducts a risk assessment if changes are deemed significant. This ensures the risks of a given change can be defined, and weighs them against the risks of not implementing the change.

Resources | The NRC has identified two areas that must be enhanced to resolve our highest priority risks: vulnerability remediation and increased coverage for the security operations center (SOC). To mitigate the first risk, the NRC is completing a project that will reduce the time needed to patch all internal workstations and servers. To mitigate the second, the current infrastructure support contract replacement will include the requirement to increase SOC capabilities and coverage, and a secondary contract will supplement operational security needs. The NRC is also taking steps to move a number of automated workflows to the cloud. The NRC will utilize FedRAMP authorized cloud services to ensure cost efficiencies are realized and to reduce costs for continuous monitoring. This approach will allow the NRC to focus on vulnerabilities and threats to systems and data that directly support the agency's HVA and Mission Essential Functions.

If funding is needed for a mitigation activity, the CIO works with the Information Technology Portfolio Executive Council (IPEC), which balances the costs and risks of the activity, and determines whether the activity will be funded.

Leadership | The NRC's senior leadership takes an active role in the management of cybersecurity risks, which are taken into consideration in the agency's broader enterprise risk assessment process required by Circular A-123.

The NRC CIO conducts a daily cybersecurity risk meeting with staff across the agency to discuss the current threat environment, prioritize cybersecurity risk management activities and continuously improve the agency's cybersecurity posture. These discussions center around available intelligence about emerging threats, existing mitigations, ongoing projects affecting the NRC's susceptibility to the threats, and the efforts needed to reduce the risk to an acceptable level.

The CISO also meets with System Owners and their Information System Security Officers to develop an understanding of the risks to their systems and data, and to outline any existing mitigation strategies and residual risks for presentation to the Authorizing Official.

Cybersecurity performance is reviewed quarterly in program performance reviews by the Executive Director of Operations. These reviews discuss the agency's achievement of strategic and performance goals and metrics with senior office managers in the context of enterprise and program risks and accomplishments. The security risks deemed agency-wide and/or of strategic interest are referred to the Executive Committee on ERM and the Programmatic Senior Assessment Team for evaluation and determining whether adjustments or additional efforts are needed to appropriately manage the risk.

Inspector General Assessment

The OIG determined through independent review that the agency has an effective information security program. NRC has made significant improvements in the effectiveness of their IT security

program, and continues to make improvements in performing continuous monitoring activities. NRC's successes include:

- The reduction of patch times resulting in a 50% reduction in vulnerabilities over the past 12 months;
- The remediation all but 3 FY 2016 IG recommendations
- Significant improvements in oversight of contractor systems; and
- The completion of security assessments and authorization for 7 of 10 subsystems of the NRC general support system.

The IG's independent evaluation identified the following IT security program areas that need improvement:

1) IT security program documentation, including policies, processes, procedures, guidance, standards, and templates are not up-to-date; and

2) Some continuous monitoring activities were not performed as required. Specifically, some security categorizations, contingency plans, and BIAs are not updated annually as required.

FY 2017 Annual Cybersecurity Risk Management Assessment

Nuclear Waste Technical Review Board

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	At Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Nuclear Waste Technical Review Board (NWTRB) categorizes cybersecurity risks based on the incident classification patterns outlined in the Verizon Data Breach Investigations Report. NWTRB's cybersecurity risks include crimeware, cyber espionage, denial of service, insider or privilege misuse, physical theft or loss, and web application attacks.

Strategy | NWTRB's strategy aligns with the overall ERM process through its internal control processes such as documented polices, IT controls, and continuous process improvement. NWTRB prioritizes risks based on the probability and impact of each threat event. NWTRB's risk response to cybersecurity threats is to mitigate or transfer, where possible, and avoid if necessary and able. The agency accepts risk only if strategic and operational value is low and budgetary cost to mitigate or transfer is too high. NWTRB has controls in place to mitigate the vast majority of identified threats, and the agency has transferred the risks associated with denial of service.

Resources | NWTRB has not aligned resources toward the acquisition of penetration testing services for cybersecurity control evaluation. Additionally, the agency seeks training to better educate the user base on the use of services to drive overall cybersecurity posture improvement.

Leadership | NWTRB senior leadership determines requirements and criticality of cyber resources, which drives the direction of the agency cybersecurity risk management strategy. Senior leadership is apprised of specific risks as needed when there are major or anticipated major shifts in the threat landscape.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for NWTRB was not performed for FY 2017, 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. Nuclear Waste Technical Review Board will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Occupational Safety and Health Review Commission

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Occupational Safety and Health Review Commission (OSHRC) has taken several steps to address risks to its case management and e-filing system, which is the agency's only mission essential function. OSHRC moved this system from email and being locally managed to a fully integrated electronic filing system housed by a FedRAMP-certified host. This solution has enhanced OSHRC cybersecurity, but the agency lacks sustained fiscal resources to staff its Information Technology Office (ITO). Current staffing permits level 2 support from 7:00 am through 4:30 pm to address user lockouts and submission issues.

These fiscal constraints limit OSHRC's ability to operate its e-filing systems continuously, and impact the ITO staff's ability to receive training to refresh their skills. OSHRC does not have a lab or development environment to test solutions prior to deployment, which increases the potential for cybersecurity pitfalls to remain following deployment into production.

Strategy | OSHRC's ITO, along with the SAOP, monitor the implementation of the agency's directives, policies, and standards as they relate to IT. OSHRC is attempting to address cybersecurity risks to its systems, although these efforts depend on fiscal resources.

OSHRC maintains memoranda of understanding (MOU) with the DHS and external agencies that house OSHRC's personnel and financial data. OSHRC's MOU with DHS allows them to scan for vulnerabilities. OSHRC also uses a limited set of local tools, including antivirus software, patch management, web filtering, redundant firewalls, and other tools deemed appropriate to scan the network for unauthorized software. OSHRC maintains current cybersecurity policies, including a recent update of its breach response plan to incorporate procedures.

In addition, OSHRC provides annual in-house security and privacy-refresher training to all Federal and contractor staff to facilitate identification of any potential hazards and to encourage a safer computing environment. Each OSHRC employee has been issued and uses a PIV card to connect to systems locally and contractors are required to access the network using fingerprint scans.

Resources | OSHRC does not have redundant connections to the internet, creating a single point of failure. Insufficient bandwidth creates a choke point for internal users. OSHRC needs resources to invest in additional third-party solutions to enhance information security for safeguarding computer networks and devices. Adding front-end filters would lower but not eradicate these cybersecurity risks. Additionally, OSHRC is awaiting initial rollout of the DHS CDM program dashboard initiative in the first half of FY 2018.

Presently, OSHRC is using its limited resources to actively monitor and update antivirus software; securely back up data on a local device and then push the data to a secure cloud host; and use shadow copy for quick recoveries in the event of accidental deletes, etc. OSHRC currently uses automated tools to provide updated software and hardware inventories. OSHRC has instituted an IT Strategic Plan that addresses a plan of action for the next five years that includes periodic software and hardware upgrades.

Unprotected or outdated systems are not the only source of security vulnerabilities at OSHRC. The actions and conduct of internal users also put OSHRC at risk of an attack or data breach. Although OSHRC is in the process of updating its training to include information about its updated breach response plan, resources for additional external cybersecurity awareness and training would help mitigate these potential threats.

Leadership | The OSHRC Chairman, along with the SAOP, ensure that the agency appropriately implements the policies, principles, standards, guidelines, rules, and regulations required by the OMB, and submits annual evaluations, along with program reviews, to the Director of OMB. The CIO is responsible for establishing a computer security program that includes, among other things, a general support system, security plans, continuity of operations, disaster recovery plan, and system authorization to operate.

Inspector General Assessment

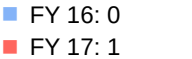
An independent evaluation of the status of the IT cybersecurity program for Occupational Safety and Health Review Commission was performed by an independent evaluator for FY 2017 and while the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have 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 IG portion was realized in FY 2017 and will continue when funding is available.

FY 2017 Annual Cybersecurity Risk Management Assessment

Office of Government Ethics

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	1
Other	0	0
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | Like other organizations, the Office of Government Ethics (OGE) faces risks of data center loss or website outage. OGE mitigates these risks by maintaining security best practices, performing weekly preventative maintenance, and proactively managing built-in security-controls. OGE maintains system awareness through Managed Trusted Internet Protocol Services alerts, weekly NCATS scans, virus scans, internal vulnerability scans, and other independent assessments.

Strategy | OGE's risk management process documents the organization's risk management decisions. Risk management is the result of intense collaboration among system managers, system administrators and developers, system owners, the CIO, and the authorizing official.

High and medium vulnerabilities are assessed and mitigated in a timely manner. If the risk management team decides to accept a risk, the system/project manager is responsible for providing the justification and the compensating control. It is a requirement that a compensating control (or sufficient justification) is defined in order to obtain full approval for a risk acceptance. Risk acceptance requires the approval of the system owner, the CIO, and the authorizing official.

Resources | OGE may fail to meet cybersecurity and IT refresh targets due to legislative and/or political risk.

Leadership | OGE is implementing the recommendations and requirements of OMB Circular A-123. OGE convened a meeting of its entire executive staff to create an agency risk registry which includes a description of a given risk, an assessment of the risk's inherent likelihood and impact, a description of ongoing mitigation strategies, an assessment of residual risk, and a description of any further mitigation efforts required to bring the risk into tolerance. Each risk is assigned to an appropriate agency leader, manager, or employee. Progress on active risk mitigation will be addressed during regular twice-annual organizational performance reviews and at periodic meetings of OGE's executive staff. Senior management is actively engaged in the ERM process, which includes collaboration with the CIO regarding the cybersecurity risk management strategy. OGE plans to update its risk registry on an annual basis.

Inspector General Assessment

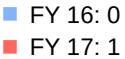
An independent evaluation of the status of the IT cybersecurity program for Office of Government Ethics was not performed for FY 2017 and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. OGE conducts a full independent cybersecurity assessment on a 3-year cycle, with self-assessments during the interim. The last full independent assessment was conducted in FY 2015. A full independent assessment is scheduled for FY 2018. Going forward, OGE plans to conduct annual independent reviews of a subset of controls over a two-year period, followed by a full reviews every three years.

FY 2017 Annual Cybersecurity Risk Management Assessment

Office of Navajo and Hopi Indian Relocation

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	At Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	1
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Office of Navajo and Hopi Indian Relocation's (ONHIR) primary risks are lack of the security content automation protocol program and lack of implementation of PIV cards for network access.

Strategy | ONHIR is a sunset agency that anticipates closing by September 30, 2018. ONHIR has applied a series of physical security controls for its Main and Field offices to limit access to the facilities and information systems. The top priority is to complete the project of PIV usage.

Resources | As ONHIR sunsets, it faces a shortage of staff to oversee its cybersecurity program. Additionally, the agency has not replaced older equipment due to our shutdown plans. The ONHIR does not have sufficient staff resources to test and implement the security content automation protocol program.

Leadership | ONHIR's Executive Director is involved in risk management plans and the development and implementation of necessary strategies. The Executive Director reviews and approves all policies and procedures before they are final. He also reviews all FISMA documents every three years or sooner if needed and signs off before sending any to the OMB. The Executive Director also attends all cybersecurity training, along with the 30 other staff of the agency.

Inspector General Assessment

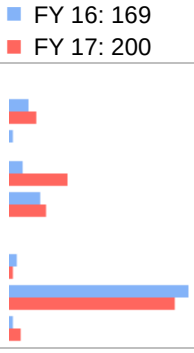
An independent evaluation of the status of the IT cybersecurity program for Office of Navajo and Hopi Indian Relocation was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. Office of Navajo and Hopi Indian Relocation will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Office of Personnel Management

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	13	18
External/Removable Media	2	0
Improper Usage	9	38
Loss or Theft of Equipment	20	24
Physical Cause	NA	0
Web	5	3
Other	117	109
Multiple Attack Vectors	3	8



CIO Risk Management Self-Assessment

Risks | Risks to OPM systems across the NIST Cybersecurity Framework functions are considered to be managed risks, including risks to HVAs and to mission essential functions. The managed risks include:

- Lack of a plan and timeline to enforce the new systems development lifecycle policy on all of OPM's system development projects. Such a plan should include improved inventory, patch management, Plan of Action and Milestones tracking and centralization, as well as other risks presented to systems through traditional lifecycle management;
- Incomplete implementation of all of the intended requirements outlined in the NIST SP 800-39, section 2.3.2 Risk Executive (Function);
- Inability to ensure that all ISAs are valid and properly maintained;
- Failure to test the contingency plans for each system on an annual basis;
- Failure to ensure whether or not clauses on the protection of information are included in contracts handling sensitive information; and
- Incomplete development of an Insider Threat Program.

Strategy | OPM employs several risk management processes to address these risks. The agency established a Risk Management Council (RMC), which is responsible for implementing, directing, and overseeing implementation of OMB Circular A-123 and all the provisions of a robust process of risk management and internal control. As the RMC is in its infancy, the implementation plan has been developed; however, a full strategy has not been completed.

On a system-by-system level, identified risks are assessed based on determining factors including type of threat or vulnerability identified, likelihood of the threat being exploited and the impact of a successful exploit of the vulnerability to the agency. Additional factors include compensating controls in place to reduce the risk, OPM cybersecurity network access controls, intrusion detection systems, data loss prevention, endpoint protection, and OPM's implementation of and participation in the DHS CDM Program. Additionally, OPM utilizes a methodical approach of a Plan of Action and Milestones process for capturing and overseeing the resolution of identified weaknesses and reducing the risk to OPM systems and data.

Resources | OPM is lacking human resources capabilities, and has had difficulty retaining and backfilling cybersecurity positions. OPM's cybersecurity staff must balance routine work responsibilities with a high volume of internal and external audits, assessments, and engagements. The availability of staff to facilitate those engagements is limited, as are the resources needed to respond to observations, documentation requests, and other interviews.

Cybersecurity technical gaps for FY 2017 and remediating tools for FY 2018 were recently identified with the Major IT Business Case. OPM communicated those budget needs to OMB.

Leadership | OPM agency senior leadership provides support and communication for the development and ongoing implementation of the agency's cybersecurity risk management strategy. The role of senior leadership, as part of the RMC, is to make strategic decisions at the enterprise level. The RMC is in the process of developing an initial OPM risk profile, which will define enterprise and cybersecurity risks.

Integration and development of the strategy into cybersecurity processes and procedures will continue under the guidance of the OPM CISO as the risk profile is finalized. During this process, OPM follows the NIST RMF for risk management decisions throughout system authorization. Senior leadership is also involved in our incident response activities as appropriate. Roles and communications are outlined in the OPM Cyber Protection and Defense Manual.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. While the overall assessment by the OPM OIG rates the OPM program at maturity Level 2 – Defined, a number of NIST Cybersecurity Framework functions were rated at Level 3 – Consistently Implemented and Level 4 - Managed and Measurable. The assessment also noted significant progress in several areas. This is the first time the OIG has utilized the maturity model in an audit of the OPM CIO, thus creating a new baseline for collaboration and discussion between the OPM CIO and the OIG.

OPM acknowledges that the agency has not consistently implemented policies and procedures, and the OIG assessment finding and recommendation reflects this. The agency has made consistent and deliberative efforts to reach Level 3 – Consistently Implemented for the Protect function and Level 4 – Managed and Measurable for Respond function. The agency will continue to address the OIG recommendations and utilize them to meet or exceed Level 3 – Consistently Implemented.

FY 2017 Annual Cybersecurity Risk Management Assessment

Office of Special Counsel

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	1	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Office of the Special Council (OSC) continues to develop and refine its ERM plan to increase the security and resiliency of the agency's IT systems and ensure compliance with FISMA requirements and NIST guidelines. OSC has focused attention and resources on fiscally sound improvements and investments in IT equipment, services, and staffing with an overarching goal of identifying and mitigating cybersecurity risks. This 360-degree review has identified the need for OSC to adopt the NIST-based RMF and take actionable steps to deal with the potential issue of data leakage and data spillage. OSC has already implemented projects to improve network security by replacing archaic firewalls and network hardware, software, and services, such as intrusion detection and prevention systems. Digital Rights Management, protection of PII, and data integrity are several areas that still require attention to reduce potential issues. One gap OSC identified is the need to complete Multi-Factor Authentication to ensure increased end-user accountability and system security requirements.

Strategy | In FY 2015, OSC engaged in an end-to-end review of its IT systems, with the primary goal to modernize and protect legacy systems while also replacing them with more secure, streamlined, and effective systems. Substantial work has been completed in that area and one of the principal action items resulting from the review was the creation of an Enterprise Risk Management Council (ERMC) to ensure the agency's executives and system owners protect the identity and privacy of customers and investigations by implementing and actively monitoring standard security controls in IT systems. Moreover, OSC has achieved many milestones pursuant to OMB IT modernization directives and the NIST Cybersecurity Framework.

During FY 2016 at FY 2017, OSC accelerated infrastructure and line-of-business projects to further enhance IT security, agility and resiliency, while reducing expenses associated with supporting legacy systems. OSC also incorporated the NIST-based RMF in the design of new products and services, ensuring the security of all new projects and procurement initiatives. OSC is also taking steps to implement additional user and object rights to help secure files, which will further enhance the protection of the agency and complainants' confidentiality and privacy requirements. Finally, OSC has been providing mandatory web-enabled cyber security training to 100 percent of personnel and contractors.

Resources | OSC's CFO is working to set aside funding for increased investments in areas identified as High Risk and At Risk in FY 2018 and beyond, and capture the needs of an ever-evolving IT environment and fully address known program risk areas. Planning is underway to implement multi-factor authentication across our entire information architecture using the prescribed GSA guidelines in 2018.

Leadership | The ERMC Charter ensures the Committee fulfills its oversight and governance responsibilities, including the development and monitoring of a risk profile and key strategic, regulatory, operational and financial risks. The ERMC is composed of senior agency managers, ensuring that the agency has a strong commitment to a risk governance structure and permits OSC's leadership team to make risk-informed decisions about resource allocation, policy and operations. OSC also established a Committee for IT (ComIT), a partnership between members of OSC's program staff and the ITB. ComIT works to improve planning, training, and communication about technology issues affecting the agency. ComIT sends agency-wide updates on OSC technology efforts and assists ITB in the development of training plans for new equipment and programs. It also coordinates an early adopter program, using volunteers from across the agency to test new technologies, ensure that they meet the needs of all OSC units, and increase end-user adoption.

Inspector General Assessment

This report presents the results of the annual FISMA IG audit. OSC underwent an audit based on FY 2017 IG FISMA Reporting Metrics provided by DHS and OMB. During this time, the Department of Interior's (DOI) Information Systems Security Line of Business (ISSLoB) interacted with OSC personnel and reviewed evidence and artifacts in order to assess the implementation of OSC's agency-wide information security program and its current security posture.

The FY 2017 IG FISMA Reporting Metrics included security controls and requirements for the following domains: Overall, Identify (Risk Management), Protect (Configuration Management, Identity and Access Management, and Security Training), Detect (Information Security Continuous Monitoring), Respond (Incident Response, Recover (Contingency Planning).

The audit showed that OSC has effectively complied at a "Managed and Measureable" level with most of the security control requirements reviewed during the audit. Moreover, OSC achieved an overall "Effective" rating.

ISSLoB provided four recommendations for OSC to consider and implement in FY 2018, including: 1) improve access controls, 2) increase utilization of system automation, 3) enhance the

cybersecurity tools kit, and 4) continuously evaluate and update the agency's business continuity and planning procedures.

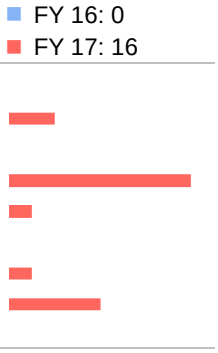
It is ISSLoB's professional opinion, and based on the results of the security audit, that OSC has effectively complied at a Managed and Measureable level with most of the security control requirements reviewed during the audit of the OSC information security program and OSC GSS information systems.

FY 2017 Annual Cybersecurity Risk Management Assessment

Office of the Comptroller of the Currency

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Not Applicable
Protect	Managing Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	Managing Risk	Not Applicable
Recover	Managing Risk	Not Applicable

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	2
External/Removable Media	0	0
Improper Usage	0	8
Loss or Theft of Equipment	0	1
Physical Cause	NA	0
Web	0	1
Other	0	4
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Office of the Comptroller of the Currency (OCC) has determined that its cybersecurity risks include:

- Nation state threat actors or cybercriminals targeting sensitive information for exfiltration and ransomware attacks; and
- Agency personnel mishandling or misusing agency information resources.

Strategy | To address the risk of nation-state threat actors and cybercriminals targeting sensitive information, the OCC conducts weekly network asset scans and bi-monthly penetration tests. OCC initiated an enterprise baseline configuration program to support standard and improved secure configuration of IT assets. An OCC FY 2018 initiative will fund expanding cloud services, redesigning data storage and retrieval solutions, and expanding mobile capabilities to reduce mission dependencies on legacy IT structures.

Through the DHS CDM Program, the OCC will gain real-time visibility into all network-connected assets and expand its cyber-detection capabilities through the DHS rollout of additional tools.

As most ransomware attacks are delivered via email, the OCC has strengthened its phishing awareness outreach efforts to the workforce, deployed an email reporting button to simplify user reporting of suspicious email, and is improving its email hygiene capabilities through its move to O365 email cloud services. Additionally, an OCC Cyber Defense Center provides 24/7 incident monitoring and response capabilities.

The OCC relies on a combination of technical and operational controls to manage this risk of agency personnel mishandling or misusing agency information resources. The OCC strictly limits the use of removable media to approved, closely tracked exceptions. Finally, it operates an active security/privacy awareness and training program that includes bi-monthly phishing exercises that provides “phished” users with additional training. In addition, the OCC has in place mature process to review and adjudicate any data incidents to include a Data Breach Reponses plan and team.

Resources | A multiyear initiative to migrate all OCC systems to Information Security Continuous Monitoring and Ongoing Authorization (OA) is funded in its current Capacity Based Operating Plan. Funding was provided for a mix of FTE and contractor Information Systems Security Officers to support this initiative. Hiring and contract activities are underway but not complete. Resources to support these efforts have active senior leadership support for inclusion in our FY 2018 budget.

The CIO, in partnership with the Office of Human Capital, is designing a Cybersecurity Workforce Strategy to implement the requirements of the Cybersecurity Workforce Assessment Act of 2015 and to adopt the NIST National Initiative for Cybersecurity Education (NICE) framework as a means to develop cybersecurity expertise in its personnel.

Leadership | Cybersecurity risk management involves senior leadership as follows:

(1) Senior Deputy Comptrollers (SDCs) authorize OCC major information systems for operation. The CIO authorizes general support systems. Authorizing Officials (AOs) are briefed on annual assessment outcomes and Authority to Operate renewal activities, with expanded risk management tasks under Information Security Continuous Monitoring/OA.

(2) A senior executive subcommittee that includes most AOs oversees CIO activities carried out in support of OCC strategic plan and priorities. Subcommittee activities include IT budget planning and decisions, major IT investments/enhancements, and additional funding requests for major projects and infrastructure initiatives.

(3) The Comptroller and SDCs receive twice-monthly briefings on cybersecurity/privacy activity across OCC defense layers.

Inspector General Assessment

For FY 2017, the Treasury IG performed test procedures at the agency level for six bureaus; the OCC was not one of the selected bureaus. As such the IG assessment section is marked “Not Applicable”. The OCC is coordinating with the Treasury OIG to ensure that the FY 2018 FISMA Audit includes a specific evaluation of OCC’s Information Security Continuous Monitoring maturity levels across the eight NIST Cybersecurity Framework domains.

FY 2017 Annual Cybersecurity Risk Management Assessment

Overseas Private Investment Corporation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	2
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	7	8
Physical Cause	NA	0
Web	1	1
Other	1	3
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Overseas Private Investment Corporation (OPIC) faces cybersecurity risks similar to those of most other organizations: system and data availability risks from malware infection and cleanup, data theft, and confidentiality and integrity risks from cyber threat actors and malicious insiders. These risks are real and ever increasing in prevalence and complexity.

OPIC is a small Federal agency and a self-sustaining financial institution that provides loans and insurance, mobilizing private capital to help solve critical global development challenges. Our overseas presence, influence, and impact make OPIC a target, both of state-sponsored threat actors and cybercriminals; these remain the most significant cybersecurity risks to our systems and data.

OPIC IT systems support and enable our mission and their availability and integrity is susceptible to compromise by dedicated adversaries. OPIC would experience significant reputational impact if the non-public information stored in these systems was stolen, altered, or exposed to an unauthorized audience.

OPIC's primary exposures come from our use of cloud services. While cloud and external service providers enable us to reduce our local infrastructure and maintenance costs, outsourcing also reduces our visibility and auditing capabilities. Depending on the provider and the service, our network sensors or audit log feeds have diminished value or are unavailable for the environment. These capabilities are heavily dependent upon the provider, and many providers do not allow or enable easy access to audit logs for automatic ingestion into our security log collection and correlation system or deployment of monitoring solutions in their infrastructure.

OPIC has explored and continues to explore the technical and managerial controls and capabilities to reduce the risk to our systems and data. The protection of this and other sensitive, non-public information either entrusted to us or produced by us is our primary concern. We anticipate deploying more robust Data Loss Prevention technology to restrict PII storage to designated repositories and to better identify and prevent unprotected SPII from leaving OPIC.

Strategy | OPIC's strategy for ERM utilizes a two-pronged approach for Risk Event Identification:

1) The OPIC Vice Presidents identify Risk Events through their knowledge and assessment of mission critical functions and bring these risks to the attention of the Enterprise Risk Committee (ERC) for discussion, or

2) The ERC holds facilitated discussions about these Risk Events and evaluates the events through a framework that covers reputation, strategic, financial, operations, reporting, and compliance at the time the risk is identified and after mitigation activities are complete.

OPIC uses a multi-step Risk Implementation Process consisting of identifying, analyzing, managing, and monitoring risks and risk responses. The ERC assigns scores to risk events, and may opt to accept the risk with the understanding that mitigation efforts brought the risk level within a suitable range; monitor if the risk is at an acceptable level and maintain awareness on the Risk Profile or; archive the risk event if determined mitigation steps have rendered it non-relevant.

Leadership | OPIC's senior leadership takes an active role in the development and implementation of OPIC's cybersecurity risk management strategy. OPIC executives have integrated cybersecurity risk as a critical component of the agency's broader ERM approach. The President and CEO, and the Board of Directors have a low risk tolerance for activities that could negatively impact the confidentiality and integrity of OPIC's data, or affect legal and regulatory compliance. The Vice President of the Department of Management and Administration, the CIO, and the CISO advise and support OPIC's President/CEO, as well as the Board of Directors' Risk and Audit Committees, on matters of cybersecurity risk management, and make determinations of resource allocation to address and prevent agency exposure to cyber risks.

Inspector General Assessment

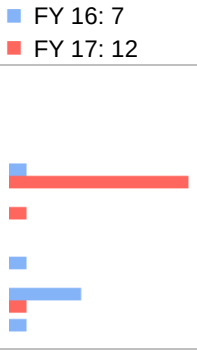
OPIC's information security program was evaluated as part of the FY 2017 FISMA audit. This audit included an evaluation of selected controls from all three of OPIC's FISMA reportable systems. The FY 2017 audit noted that 98 of 104 selected NIST 800-53, Revision 4, security controls were properly implemented. This led to the determination of OPIC having an overall effective information security program. There were three recommendations made to help OPIC improve their information security program. A full list of recommendations can be found in the FY 2017 FISMA audit report.

FY 2017 Annual Cybersecurity Risk Management Assessment

Peace Corps

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	1	10
Loss or Theft of Equipment	0	1
Physical Cause	NA	0
Web	1	0
Other	4	1
Multiple Attack Vectors	1	0



CIO Risk Management Self-Assessment

Risks | The protection of the Peace Corps' volunteers' private data are agency priorities. Therefore, information systems supporting those priorities must remain operational. Based on our latest assessment, the three most significant technical risks derive from deficiencies in Identity Assurance/Privilege Management, Software Asset Management and Vulnerability Management. In addition to those technical risks, Peace Corps has an issue with maintaining a skilled workforce, primarily due to the five-year term limit for staff. The inability to staff adequately keeps critical systems at risk due to lack of knowledge retention, absences, inadequate system maintenance and shifting priorities.

Strategy | Peace Corps' strategy is to mitigate the identified risks. The combination of risks above creates a scenario where it is highly likely these risks are realized. In order to address the potential for risk realization, remediation strategies were discussed with senior leadership. Funding was approved and remediation efforts are now underway.

Resources | Capabilities where funding and staff are necessary for remediation include: network perimeter (firewalls), account management processes (roles, off-boarding), software management (authorization, licensing) and vulnerability management (patch remediation). Leadership has supported resourcing and efforts are underway. The Peace Corps expect significant progress toward closing identified gaps in the next 12 to 18 months.

Leadership | Senior leadership at Peace Corps remains intimately involved in development of the cybersecurity risk management strategy. The visibility of the ERM strategy recently increased when it was elevated to an agency strategic objective. A work group has to better define ERM requirements and processes have been established so that cybersecurity risks will be reviewed at the enterprise level. Currently, cybersecurity risks are communicated to Technical Advisory Board (TAB), made up of senior leadership and critical business unit directors. The TAB reviews risks and mitigation strategies and determines whether they accept that strategy and related funding requests for resources and staff. Once a project is approved, progress is tracked in subsequent quarterly TAB meetings.

Inspector General Assessment

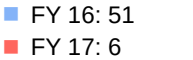
The IG assessment reflects that the Peace Corps lacks an effective information security program, as the DHS considers Level 4, "Managed and Measurable," to be an effective level of security for the overall program. Based on the assessment of the Peace Corps' information security program, the overall maturity level results are between Level 1, "Ad-hoc," and Level 2, "Defined." As such, the IG identified issues relating to the people, processes, technology, and culture aspects across all the NIST Cybersecurity Framework function areas. Moving forward, to advance and fully develop the information security program, involvement from all levels of Peace Corps leadership is needed.

FY 2017 Annual Cybersecurity Risk Management Assessment

Pension Benefit Guaranty Corporation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	3	2
External/Removable Media	0	0
Improper Usage	2	1
Loss or Theft of Equipment	27	0
Physical Cause	NA	0
Web	15	1
Other	4	2
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

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

- Delays in modernizing legacy systems to increase cybersecurity resilience;
- Continued use of technology at or near End of Service Life;
- Insufficient resources to acquire adequate cybersecurity workforce;
- Lack of an effective continuous monitoring program;
- Inadequate attention by the Corporation's workforce regarding emerging threats such as phishing, ransomware, and social engineering;
- Less than optimal security hardening of hardware and software;
- Inability to detect and prevent insider threats; and
- Excessive time to deploy security patches.

Strategy | PBGC manages its risks by developing risk mitigation plans, creating Plans of Action and Milestones, implementing mitigation plans, and accepting risks where operational constraints exist.

PBGC also employs programmatic strategies and approaches that ensure PBGC systems are compliant with the Corporation's Information Security Program and applicable laws and regulations. PBGC has established an IT RMF process to align with the NIST RMF. This PBGC RMF emphasizes managing risk at three different tiers: corporation-wide, at the business/mission processes, and within information systems.

Resources | The Corporation is planning to request additional resources for the replacement of IT Infrastructure components that have reached or are reaching end-of-service-life and present critical cybersecurity and functional risks.

PBGC will need supplemental funding for additional support staff to fully implement the NIST Cybersecurity Framework core functions.

Leadership | The ECD provides program status updates to the CIO monthly, and the CIO periodically briefs executives from each business unit about cybersecurity risks impacting their program.

The CIO sponsors the PBGC Cybersecurity and Privacy Council led by the CISO and comprised of Federal Information System Security Managers from the Corporation's business units and the Chief Privacy Officer with the goal of sharing information and making recommendations pertaining to cybersecurity to senior leadership.

Inspector General Assessment

In FY 2017, PBGC's information security program was not effective. PBGC made improvements on its entity-wide security management and access control and configuration management weaknesses but the functional areas were not at a managed and measurable maturity level. PBGC has implemented its Information Security RMF Process and filled its Risk Management Officer position, in addition to requiring strong authentication for all privileged users and almost all non-privileged users. PBGC also redefined its training program to address open recommendations which required additional cycle time to verify the effectiveness of the new monitoring process. The Corporation, however, still needs to ensure accounts are maintained in accordance with PBGC policy, unsupported software is removed, and continued focus is provided to ensure that its flaw remediation process continues to improve on the timely remediation of vulnerabilities and application of necessary patches.

FY 2017 Annual Cybersecurity Risk Management Assessment

Postal Regulatory Commission

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	High Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	At Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Commission's cybersecurity risks are similar to those seen elsewhere in the government: new and emerging threats, outdated tools to monitor and mitigate threats, and a gap in its cyber workforce.

Strategy | The Commission utilizes a structured risk management strategy that incorporates FISMA metrics and the NIST Risk Management. As a general practice, the Commission does not accept risk from known unmitigated vulnerabilities and makes every attempt to mitigate all new and emerging risks. The Commission's IT management team has developed a Risk Management Assessment & Action Plan (RMAAP) to continuously address and prioritize risks and gaps and document milestones and resources needed to guide risk management decisions. The RMAAP is reviewed with the Deputy Secretary on a weekly basis to discuss any outstanding risks and vulnerabilities, mitigation strategies, and potential resource challenges. It is reviewed with the Secretary monthly. All vulnerabilities and risks not easily mitigated and/or having budgetary impact are elevated directly to the Secretary and Chief Administrative Officer of the Commission.

Resources | The Commission's largest gap is the lack of sophisticated security tools and sensors provided by the CDM program. The full implementation of this program will help reduce the Commission's overall risk by simplifying the security authorization process, providing continuous monitoring of agency systems and IT assets, providing an up-to-date status of the Commission's security posture, and allowing senior leaders to make more informed risk management decisions. This is particularly pressing as, following a major modernization effort in FY 2017, the Commission will need to undergo ATO processes for multiple systems in FY 2018. CDM would significantly decrease the financial and personnel costs of the process, both of which have significantly slowed past security efforts such as PIV implementation.

Leadership | Due to the small size of the agency, there is a direct line of communication to senior leaders, and the entire leadership team is actively engaged in cybersecurity decisions, including those regarding funding and response to threats.

The IT Manager meets daily with Deputy Secretary of the Commission, who serves as the Senior Accountable official for cybersecurity to discuss emerging threats and mitigation strategies. The Deputy Secretary then meets daily with the Secretary, providing actionable cybersecurity briefings when threats arise. The Secretary and the Chairman of the Commission then discuss cybersecurity issues, including operational and mission impact and mitigation strategies, as part of their weekly briefings.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for the Commission was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). The Commission's OIG will explore providing this independent evaluation in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Presidio Trust

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Presidio Trust (Trust) has been, and continues to be, limited by strategic, operational, and budgetary considerations.

Strategy | One deliverable from the recently conducted risk assessment was a FISMA Implementation Roadmap. Additionally, the Trust leverages DHS's weekly perimeter network scans and quickly remediates any identified vulnerabilities. Most recently, the Trust implemented EINSTEIN 3A to augment its email and web content filtering capabilities.

Resources | Unlike the vast majority of Federal agencies, the Trust does not receive any appropriations from the Federal Government for execution of operational functions such as FISMA implementation. For these reasons, it was determined that the Trust could not comply with FISMA without compromising its financial self-sufficiency and statutory mandates, until FY 2016, which would mark the Trust's fourth year without Federal financial operating support. While operating solely on its revenues, the Trust continues to align budgetary resources with its strategic plan. In early January 2017, the Trust contracted a risk assessment to determine the Trust's compliance with FISMA, align the business to FISMA compliance requirements, and develop a roadmap outlining the strategy for future FISMA implementation.

As the organization develops its strategy to implement an enterprise-wide security program following the NIST Cybersecurity Framework, the Trust's leadership realizes there are areas that will require additional budgetary attention, increased human resources, or augmented skills and tools. In FY 2018 and beyond, considerable resources have been earmarked for the Trust's security initiatives.

Leadership | Senior Leadership has played a key role in developing, supporting and implementing the organization's cybersecurity risk management strategy. Further commitment is reflected in the Five-Year plan, and substantial consideration has been given to allocating the proper resources to both implement an enterprise-wide ERM strategy and fully comply with FISMA.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for the Trust was not performed for FY 2017, 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 Trust will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Privacy and Civil Liberties Oversight Board

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	At Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	At Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | An understaffed IT workforce represents the primary cybersecurity risk to the Privacy and Civil Liberties Oversight Board's (PCLOB) Mission Essential Functions. The OCIO cannot fill vacancies until the appointment of the Chairman of the Board, who retains hiring authority for the agency. This personnel shortage limits the ability of the OCIO to further develop the security architecture while preserving security baselines and cultivating the knowledge and skills to achieve cybersecurity goals. This risk is exacerbated by the agency's approaching relocation in the spring of 2018, which will require changes to the IT architecture, engineering and coordination for new services, and the transition of classified and unclassified information systems. Lastly, the PCLOB faces threats posed by Advanced Persistent Threats, cyber criminals, and insider threats.

Strategy | The PCLOB mitigates risks to the availability and integrity of networks and data through a strong foundational security architecture with a small public facing footprint. Currently, the agency is transitioning their c contract to the GSA Networx contract while adding redundant circuits and Managed Trusted Internet Protocol Services. Additionally, the PCLOB will implement the DHS's CDM program in early FY 2018. The agency also plans to refine policies, procedures, and training to mitigate unintended or malicious exposure of privacy protected data. Incorporation of capabilities such as data-at-rest and data leak detection tools are under analysis. Utilization of Shared Service Providers is a primary strategy to manage the remaining identified risks.

The PCLOB has entered an Inter-agency Agreement (IAA) with the Department of Interior (DOI) to enable greater agility in procurement of services to mitigate risks associated with IT workforce gaps. Through the IAA, the PCLOB released solicitations for key cybersecurity projects, including the Networx contract and for an independent third-party auditor. An IAA was also established with DOI's offerings through the Information System Security Line of Business (ISSLoB) to provide FISMA readiness support and security engineering support and to support the evolution of PCLOB's IT Risk Management program. The agency also leverages the Department of State's Security Awareness Training ISSLoB to train privileged users and to enhance the executive leadership team's understanding of FISMA requirements and responsibilities. Lastly, the agency is seeking an ISSLoB offering to augment detection, analysis, and response functions until CDM is implemented, staffing vacancies are filled, and after relocation is complete.

Resources | The principal gap identified is resources to support the maturation of cybersecurity processes, procedures, and system security plans. Financial resources have been allocated to fill this gap utilizing the DOI ISSLoB offering. The OCIO has deferred pursuing new capabilities pending implementation of Archer under the CDM program. Additional gaps include data at rest and data leak protection technologies. The PCLOB currently employs policies and processes to address these capability gaps. Based on current project schedules and availability of resources, the agency expects to address automated capabilities in FY 2019 or beyond.

Leadership | Per the OMB Circular A-123, the Board initiated programs to build and mature the agency's ERM program and established an internal control officer position, which will be filled after the appointment of the new Chairman. Internal control functions and programs are being managed by the General Counsel, the Chief Management Officer, and the CIO. In line with the broader ERM program, the Board provides governance and oversight for the cybersecurity risk management strategy. The Board is currently in a sub-quorum state resulting in temporary modifications to formerly established processes. Board Member Collins receives detailed biweekly briefings from the senior leadership team on all internal control areas. Staffing procedures have been instituted to ensure key decisions are visible and reviewed by the entire leadership team. The Board's direct and consistent involvement has resulted in significant progress in establishing institutional processes, dedicated support to build a financial controls program, and support and funding for a robust cybersecurity program that includes a FISMA support team, TIC, CDM, and many more capabilities.

Inspector General Assessment

An independent evaluation of the IT cybersecurity program for PCLOB was not performed for FY 2017, 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 Privacy and Civil Liberties Oversight Board will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

Railroad Retirement Board

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

Incidents by Attack Vector	FY 16	FY17
Attrition	0	0
E-mail	15	5
External/Removable Media	1	0
Improper Usage	18	20
Loss or Theft of Equipment	27	25
Physical Cause	NA	0
Web	0	2
Other	7	13
Multiple Attack Vectors	1	0

CIO Risk Management Self-Assessment

Risks | The Railroad Retirement Board (RRB) is experiencing challenges with its legacy systems architecture, built decades ago in a closed environment that is constantly patched rather than re-engineered. The RRB is constantly patching the insecure architecture to combat security challenges, fraud prevention and detection is a time-consuming, manual process. With the development of a replacement distributed systems environment for the legacy systems architecture, information security risks will increase and it will be critical for the RRB to implement an updated risk assessment for the new system. In addition, RRB has an IT workforce that is rapidly retiring from the agency. As a result, RRB is facing a decrease in the institutional knowledge and skills to maintain these legacy systems.

The RRB evaluates cybersecurity risks in Information Security Continuous Monitoring program of the RRB information system during a third-party assessment (DSD Labs) and from the guidance of the RRB OIG FISMA review. The updated risk assessment in September 2016 identified the following risks: conduct attacks leveraging traffic/data movement allowed across perimeter; exploit poorly configured or unauthorized information systems exposed to the Internet; compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware); Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware); obtain unauthorized access; cause integrity loss by polluting or corrupting critical data; inability to recover system.

Strategy | The RRB has implemented an Information Security Continuous Monitoring strategy that addresses the risks to the information system and ensures the authorizing official is informed to make a risk based decision for authorizing the system to operate. All weaknesses identified in the risk assessment performed by the third-party assessor, the OIG FISMA review, and other information security reviews are recorded in the agency Plan of Actions and Milestones.

The RRB manages the risk of the critical infrastructure considering asset management, remote access, identity management, and network protection using the following techniques:

- Access Management: The RRB has enrolled in the DHS' CDM Continuous Monitoring-as-a-Service (CMaaS) to provide better visibly of current hardware and software and to automatically detect unauthorized hardware and software;
- Identity Management: The RRB has a multi-factor authentication solution in place and is enrolled in the DHS CDM CMaaS and will be implementing credential management for general users and access management for privileged management;
- Remote Access: The RRB recently deployed managed services for hardware encryption and we are employing upgraded Cisco ASA firewalls to strengthen information security controls for Virtual Private Network remote access;
- Network Protection: The RRB has enrolled in the DHS CDM CMaaS to improve upon the Defense-in-Depth configuration-in-place monitoring performance metrics; and
- All IT request for purchases are requested through the agency Information Technology Steering Committee (ITSC) managed by the CIO. Once an IT initiative is approved by the ITSC, the requests are considered by the Investment Review Board (IRB).

Resources | The RRB continues to progress toward a compliant information security program improving the RRB's security posture. An Information Security Continuous Monitoring strategy has been implemented and expects CDM services to improve its Information Security Continuous Monitoring strategy pertaining to vulnerability assessment, hardware and software management, configuration management, and privileged account management. The CDM solution is scheduled to be implemented for the RRB in the beginning of December 2017. Other initiatives included enforcing multi-factor authentication for non-privileged and privileged accounts, request for procurement for an automated configuration management solution, the request for services from DHS to perform penetration testing of the RRB information system, and developing information security continuous monitoring practices.

The RRB continues to address challenges and risks, including agency budgetary challenges, staffing resources in the IT field and cybersecurity positions including application security. The RRB's goal is to decommission the mainframe at the earliest timeframe to address the legacy architecture risks.

Leadership | RRB senior leadership review and approve all information security initiatives recommended by the CISO, who works directly for and reports all information security risks to the CIO. The CIO is a member of the Executive Committee and ensures all the information security risks are addressed. The Executive Committee reports to the RRB's three-member board on all RRB matters including budget.

The Risk Management Program is included in the ERM process as required by OMB Circular A-123 as an assessable unit

required to report to the agency's Management Control Review process annually. The CISO is a member of the Management Control Review Committee as a representative for the CIO and evaluates the ERM for the RRB. In the CISO's report to the Management Control Review Committee, he identifies the risks associated with the Risk Management assessable unit and identifies opportunities for improvement.

Inspector General Assessment

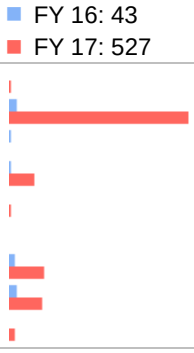
The OIG determined through independent review that although RRB implemented changes in the information security program for improvement, a fully effective security program that meets the requirements of FISMA has not been achieved. In FY 2017, RRB hired an application security program analyst to address a resource gap identified in our FY 2016 FISMA audit, successfully accomplished a data exchange with the Social Security Administration in conjunction with disaster recovery testing of a mission essential application, and entered into an interagency agreement with the GSA to use identity proofing and multi-factor authentication for all citizen centric services. Despite these improvements, RRB's efforts to implement a security program that is consistent with FISMA continues to be ineffective due to the numerous open audit recommendations related to strategy plans, policies and procedures, resource allocation, and performance metrics to evaluate and modify the program based on the evaluation results. Implementation of these critical open audit recommendations dating back to 2002 would allow RRB to meet requirements to achieve the necessary lower levels of maturity established in the maturity model developed by OMB and DHS. As a result, each of the seven OIG FISMA metric domains and the corresponding NIST Cybersecurity Framework functions have been assessed as "Not Effective" when evaluated using the maturity model.

FY 2017 Annual Cybersecurity Risk Management Assessment

Securities and Exchange Commission

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	15	336
External/Removable Media	1	0
Improper Usage	2	48
Loss or Theft of Equipment	0	2
Physical Cause	NA	0
Web	11	65
Other	14	63
Multiple Attack Vectors	0	12



CIO Risk Management Self-Assessment

Risks |

In September 2017, the Chairman of the Securities and Exchange Commission (SEC) announced that a previously-identified security incident was determined to have resulted in access to nonpublic information. As a result, the agency has embarked on an interagency initiative to increase collaboration around cybersecurity risk, increase awareness on the types and nature of all data the agency maintains within its information systems, and implement business process enhancements to external-facing systems, including EDGAR.

The SEC is also working to address risks identified by its auditors, requiring refinement of the agency's information security program planning and documentation, protocols related to configuration management, and identity and access management.

Strategy | The SEC is proactively working to address and mitigate identified deficiencies which include taking steps to improve communication and escalation protocols and enhance the information security of the EDGAR system. In addition to actively managing and remediating identified risks, the SEC focusing on web application security and the implementation of additional access control enhancements for public-facing systems.

The SEC is actively tracking the aforementioned items through management of agency plans of action and milestones with aggressive timeframes for remediation. The SEC developed an approach for managing identified cybersecurity risks in accordance with OMB directives and guidance from the NIST. The SEC tracks identified risks to information systems using Plans of Action and Milestones within the SEC Enterprise Governance and Risk Compliance (eGRC) tool. This tool allows each Plan of Action and Milestones to be updated on a regular basis and provides real-time reporting to dashboards that display Plan of Action and Milestones progress by critical factors. In addition, static reports are generated on a weekly basis and Information System Owners (ISOs) receive special notifications within 180 days of a Plan of Action and Milestones due date. Plan of Action and Milestones due dates are agreed upon by Office of Information Technology Security staff and ISOs and vary depending on the severity of the threat or vulnerability and likelihood of it being exploited.

The SEC also established a formal committee for evaluating more complex risks, primarily focusing on decisions to accept or reject critical cybersecurity risks. Technical evaluations of vulnerabilities and threats are conducted to provide senior leadership with sufficient information to make a risk based determination. The SEC has approved risk acceptances for unmitigated vulnerabilities in situations when there are compensating controls, a system has multiple layers of security protection, and there is a plan to replace a legacy system in the near future, or the cost of mitigating the risk would not be prudent based on a low probably of a risk occurring.

In July 2017, the SEC completed a number of efforts pursuant to the President's Executive Order 13800. These efforts included the development of a NIST Cybersecurity Framework implementation plan that discusses the status of the SEC's proposed internal management of cybersecurity risk using the updated metrics aligned to the Cybersecurity Framework; a timeline to map existing and planned capabilities with Cybersecurity Framework functions; and proposed uses of the terminology and concepts in the Cybersecurity Framework to organize and communicate cybersecurity activities and outcomes. The SEC plans to complete its implementation of the Cybersecurity Framework by the end of 2018.

Resources | The SEC identified gaps related to the implementation of a mature continuous monitoring program as a high priority risk. This was also a finding by both Government Accountability Office and by the OIG. To address these findings, the SEC has been working on developing a CM strategy document that covers ongoing authorization, recurring security assessments and vulnerability scanning. SEC has made investments in new tools, including transitioning to an enhanced vulnerability management capability and improving network visibility and protection mechanisms with advanced perimeter defenses. SEC is working closely with DHS to obtain and deploy the tools selected for the CDM program's Phase 1 and 2 and both agencies are working collaboratively on a custom solution that incorporate existing SEC tools.

To assist in these efforts, the Chairman authorized the hiring of additional staff and outside technology consultants to aid in efforts to protect the security of the SEC's network, systems and data in September 2017.

Leadership | Senior leadership plays a significant role in the development and implementation of the agency's cybersecurity risk management strategy. The SEC CIO and CISO play important roles with respect to key agency operational and investment bodies including capital planning, human resources, and operational risk committees. Additionally, cybersecurity risks are considered by a broad set of SEC senior officials that participate in an agency-wide risk management oversight committee (RMOC), which is responsible for monitoring the SEC's risk environment. The RMOC meets monthly, and is

comprised of SEC senior officials representing most Offices and Divisions. The RMOC serves the function of the Risk Management Council (RMC) as described in OMB Circular A-123. Further, in May 2017, the Chairman established a senior-level cybersecurity working group to coordinate information sharing, risk monitoring, and incident response efforts throughout the agency.

Inspector General Assessment

Overall, the SEC has improved some aspects of its information security program; however, additional improvements are needed for the SEC's information security program and practices to be considered effective. The auditors determined that the SEC's information security program does not meet the definition of "effective" (as defined in the FY 2017 IG FISMA Reporting Metrics V 1.0, dated April 17, 2017) because the program's overall maturity did not reach Level 4, Managed and Measurable. In FY 2018 Q2, the SEC plans to issue an audit report that will make specific recommendations to agency management to address these deficiencies.

FY 2017 Annual Cybersecurity Risk Management Assessment

Selective Service System

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	1
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	21	59
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | Selective Service System's (SSS) cybersecurity risk is driven by a lack of capital investment and full time equivalent employees. Mission essential tasks require SSS to store large amounts of PII. The agency assumes high levels of risk in the event of mobilization during a national emergency, which will significantly stress systems and require massive manpower and infrastructure expansion and increased defenses in order to work with interagency partners.

Strategy | The agency uses an ERM approach with rigorous internal controls. SSS approaches risk management using a "Cybersecurity Framework" that synchronizes agency efforts to operationalize and protect a complex relational database and data repository containing one of the largest consolidations of PII in the Federal government. The Director of Selective Service ensures an organizational approach to cybersecurity, ensuring risk management is associated with all operational lines of activity.

Our security risks are assessed against the following mission/business processes: ERM; continuous assessment and monitoring of evolving cyber requirements; capital investment and programming; acquisition and asset life cycle management; organization and structure/human capital management; program management; education and training including recurring exercise of data breech and privacy act related events; recurring reports (maintaining situational awareness); and tailoring process and procedure to emerging requirements.

Resources | Risk mitigation is a factor of capital investment and budget allocation, servicing enhanced manpower allocation and continuous monitoring of our defense in depth approach to cyber security. Development and funding for cyber security exercises supporting mobilization services during a national emergency is necessary to sustain reliable capabilities in the national preparedness community.

The agency has sustained baseline operations and cybersecurity on a flat-lined budget since 1983, and the discretionary budget shrinks in real dollars each FY. Life cycle management and software assurance is addressed in the agency's FY 2019 budget request.

Leadership | SSS's executive leadership team leads the implementation of cybersecurity risk management , the FY 2018 budget plan, and FY 2019 budget build, and ensures that operations drive the IT capital investment. Cybersecurity remains a priority line of effort for the agency. The Chief Operating Officer ensures full coordination with our CFO and logistic and contracting infrastructure to enable timely, relevant, and sustainable capital investment.

Inspector General Assessment

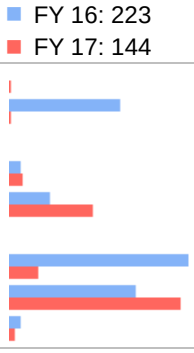
The SSS-contracted IG has concluded that SSS was in overall compliance with FISMA requirements and rated as effective. SSS IG determined that SSS had developed an agency-wide IT security program based upon assessed risk, and that their security program provided reasonable assurance, overall, that the agency's information and information systems are appropriately protected with recommendations for continuous improvements to ensure viable IT security controls.

FY 2017 Annual Cybersecurity Risk Management Assessment

Small Business Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	52	1
External/Removable Media	0	0
Improper Usage	5	6
Loss or Theft of Equipment	19	39
Physical Cause	NA	0
Web	83	14
Other	59	80
Multiple Attack Vectors	5	3



CIO Risk Management Self-Assessment

Risks | The Small Business Administration (SBA) has determined that agency data is at risk of being exposed during a cyberattack or other infrastructure compromise. There is currently a lack of enterprise-wide vulnerability management, configuration management, and asset management capabilities, resulting in an increased risk of a compromising cyberattack. Similarly, there are deficiencies and a lack of maturity around governance, account and privileged user account management, security training, log review, data rights management, and data loss prevention that is leading to an increased risk in infrastructure compromise.

Additional risks SBA identified include inadequate IT planning, procurement, and standards that may result in lack of transparency in agency-wide IT investments. There is also a lack of IT security capability maturity, which could lead to reduced network, infrastructure, and application resiliency. The agency's decentralized IT security management could result in a lack of enterprise-wide risk transparency and/or a gap in security control deployment. Finally, the existence of non-standard and legacy hardware and software may expose the agency to un-remediated security vulnerabilities due the unavailability of vendor support for these systems.

Strategy | SBA began integrating cybersecurity risk management practices into its enterprise-wide ERM process, which includes cybersecurity risks monitored by the agency's ERM Board. The ERM board monitors top-level risks associated with cybersecurity, including the potential exposure of agency data. In addition, the CIO identifies gaps in cybersecurity funding, which the ERM Board reviews.

SBA is in the process of further defining the agency's RMF structure, processes, and procedures. Once this process is complete, the agency anticipates that the CIO and CISO will have an enhanced ability to elevate cybersecurity risks to the ERM Board.

Actions are underway to mitigate risks identified through the ERM process. These risks include deployment of the DHS' CDM program and deployment of enhanced patch and configuration management processes and technologies. SBA is also monitoring deployment of Data Loss Prevention technologies, the decommissioning of unsupported hardware and software, and the migration to the cloud, advancing disaster recovery capabilities.

Resources | SBA is currently deploying DHS's CDM program, to mitigate many agency risks, including vulnerability management, configuration management, asset management, account and privileged user management.

IT management capabilities will continue to mature as governance and transparency are enhanced. Activities are underway to implement collaborative, enterprise-wide information security management of decentralized systems and assets. The agency is implementing a number of tools and technologies for log review, data rights management, and data loss prevention as we migrate to the Microsoft Azure Cloud environment. Implementation of the Microsoft Office 365 environment, including Microsoft OneDrive, will mitigate some risks.

Through continuous process improvement, SBA is aligning individual HVAs and mission essential functions more closely to risks.

Leadership | The SBA ERM process is based on, and is compliant with, OMB Circular A-123. The SBA ERM Board is comprised of 16 members from each of the major program offices, with SBA's Deputy Administrator serving as the Chairman and the Chief of Staff serving as the Vice Chairman. Agency senior leadership is involved in the management of all cybersecurity risks submitted for review and/or accepted by the ERM Board.

The primary responsibility of the Board is to understand the most significant risks facing SBA, and ensure risks are addressed in a timely manner. The SBA ERM meets monthly and reviews the entire risk list. All enterprise risks are re-baselined and validated annually. The ERM Board influences agency budgets based on agency enterprise risk.

Inspector General Assessment

In accordance with the FISMA, we evaluated the design, implementation, and operating effectiveness of SBA's information security policies, procedures, and practices. Specifically, we assessed the maturity of SBA's information security program, as outlined under the FY 2017 IG FISMA reporting metrics, and tested against these metrics by selecting a subset of 11 systems and evaluating them against the guidance outlined in FISMA. Based on these results, we determined that SBA's maturity level generally was at a Level 2 "Defined" level. Using the maturity level ranking criteria, we determined that the agency's security program is not effective.

We made 10 new recommendations in the following FISMA domains: Identify (3), Protect (4) and Recover (3). These are in addition to the 23 open FISMA recommendations. While SBA has worked to implement recommendations from previous FISMA

reports, challenges remain in implementing an effective IT security program.

FY 2017 Annual Cybersecurity Risk Management Assessment

Smithsonian Institution

Framework	RMA Rating	IG Rating
Overall	Not Applicable	
Identify	Not Applicable	Ad Hoc
Protect	Not Applicable	Defined
Detect	Not Applicable	Defined
Respond	Not Applicable	Defined
Recover	Not Applicable	Ad Hoc

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	7	3
External/Removable Media	0	0
Improper Usage	2	2
Loss or Theft of Equipment	8	3
Physical Cause	NA	0
Web	7	6
Other	8	10
Multiple Attack Vectors	4	0

CIO Risk Management Self-Assessment

Smithsonian Institute did not submit a self-assessment of their risk management risks, strategy, resources, or leadership and did not receive a risk management rating.

Inspector General Assessment

Williams Adley selected two moderate impact Smithsonian Institution systems, Smithsonian Astrophysical Observatory (SAO) Scientific Computing Infrastructure (SCI) and SAO High Energy Astrophysics (HEA), to perform detailed testing for the FY 2017 FISMA audit.

Based on our discussions with Smithsonian Institution personnel and inspection of the supporting documentation, the Smithsonian Institution has not fully developed strategies and plans for most FISMA domains. In addition, the Smithsonian Institution has not fully defined information security related policies and procedures for the two selected systems.

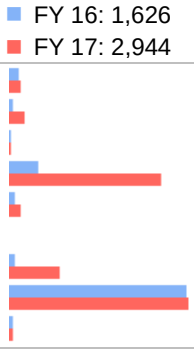
The DHS considers Level 4, “Managed and Measurable,” as an effective level of overall security program. Based on the assessment of Smithsonian Institution’s information security program, the overall maturity level falls between Level 1, “Ad-hoc,” and Level 2, “Defined” and is therefore not effective.

FY 2017 Annual Cybersecurity Risk Management Assessment

Social Security Administration

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	69	81
E-mail	26	112
External/Removable Media	1	5
Improper Usage	196	1,059
Loss or Theft of Equipment	43	79
Physical Cause	NA	0
Web	40	349
Other	1,224	1,236
Multiple Attack Vectors	27	23



CIO Risk Management Self-Assessment

Risks | Administering the Social Security Administration (SSA)'s programs requires it to collect PII for approximately 325 million Americans. This information is vital to performing the agency's essential functions but makes its network, systems, and databases a value-rich target for adversaries. SSA's greatest cyber risk is a breach of data leading to a major loss of citizen PII. A 2016 incident response exercise estimated that a major breach of agency data would cost the Federal Government $750 million and affect over 60 million Americans.

SSA's early adoption of IT and automation contributes to its modern day vulnerability to attack. Significant amounts of legacy software and infrastructure are now unsupported with fewer automated protections for vulnerability and configuration management. The skills needed to maintain these aging systems have also become scarcer and the effort greater. SSA has developed an IT Modernization Plan to address this risk.

Locally developed applications, created to increase local efficiency, pose additional risks because they lack the risk management and security processes designed for mission essential systems.

Strategy | SSA established an ERM Profile for prioritizing risks that affect its mission and operations, identifying cybersecurity as one of its highest enterprise risks. To support SSA's ERM Profile, a detailed Cyber Risk Register was created to record and prioritize cybersecurity risks. The Register provides a comprehensive view of risks identified through security reviews, external audits, third party testing, and government-wide performance measures. Overall risk exposure is determined based on likelihood, potential impact to business functions, and presence of compensating controls.

Risk mitigation strategies are developed by evaluating alternatives and considering a range of factors, including security benefit, cost, human capital needs, availability of resources, and impact on competing cybersecurity priorities. Also considered are the technical impact on SSA's network and IT assets, the effect on related business processes, and any additional user burden. Decisions to accept risk, made by evaluating the aforementioned criteria, are documented as part of an action plan to address cyber risks.

Resources | SSA has identified high priority risks in its Identify and Protect capabilities, and has made an effort to increase budgets for these areas.

In the Protect function, while SSA has encrypted most of its end point devices, cloud servers and storage, and mainframe storage, work still remains. Additionally, the agency is implementing network segmentation to limit the exposure of sensitive data in the event of unauthorized access. SSA is also deploying a privileged access management solution to further protect privileged accounts and prevent compromise.

In the Identify and Protect functions, opportunities exist to further automate the identification and mitigation of software-based vulnerabilities during the development process. Additional efforts will provide integrated and interoperable access control solutions needed to migrate legacy systems to cloud-based environments.

Also in the Identify function, SSA will implement new capabilities to strengthen its management of "shadow IT". The agency will continue to implement strong risk management for all agency software, including improving software asset management capabilities through the CDM program.

Leadership | SSA has consolidated its major NIST Cybersecurity Framework functions under the authority of the CIO and CISO. The agency provides senior executives and other relevant leadership with awareness of high priority cybersecurity risks using tools such as its ERM Profile, Cyber Risk Register, and weekly, monthly, and quarterly briefings, including to the Acting Commissioner.

Additionally, SSA's senior leadership plays a direct role in allocating cybersecurity resources. The CIO approves the agency's cybersecurity budget request as part of the agency's President's Budget Year budget formulation process. Approval of cybersecurity resources is approved via an executive-level Investment Review Board, which requires multiple levels of staff and executive management reviews.

Inspector General Assessment

Although SSA had established an agency-wide information security program and practices, we identified a number of control deficiencies related to Risk Management, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning. The weaknesses identified may limit the agency's ability to adequately protect the organization's information and information systems.

SSA IG did not assess any of the individual reporting metrics or overall FISMA domains as Managed and Measurable (Level 4). SSA was rated as 'Not Effective', as FY 2017 FISMA IG

Reporting Metrics defines an effective information security programs as at least Managed and Measurable (Level 4).

FY 2017 Annual Cybersecurity Risk Management Assessment

Surface Transportation Board

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Surface Transportation Board (STB) maintains several unique, high-valued programs and databases that support mission essential functions, two of the most critical being the Uniform Rail Costing System (URCS) and the Waybill data. Each are critical to the STB operations, and current risks such as ransomware attacks, malware, insider threats, and loss of availability of the assets are the primary risks to these assets.

The STB performs routine internal risk assessments, and has established procedures for performing risk assessments in response to cybersecurity incidents. These *ad hoc* risk assessments help the STB determine the cause of an incident, as well as actions needed to protect against future occurrences. Although a formal, full-risk assessment has not been performed at the STB since becoming an independent agency, the STB is currently undergoing an annual FISMA audit.

Strategy | STB is transitioning its IT enterprise from legacy enterprise, which is government-owned and operated, to a cloud-based enterprise. The STB will leverage the many advantages of cloud-based technologies as described in the Federal Cloud Computing Strategy to provide state-of-the-art information management services to the STB staff and its stakeholders. The STB intends this migration to facilitate improved agency operations as well as meet Federal Continuity of Operations (COOP) requirements.

Resources | Currently, the biggest gap is in the STB's ability to efficiently detect changes to its infrastructure. The STB utilizes a number of systems that collectively audit most changes to the STB infrastructure. However, these systems do not provide sufficient coverage to effectively identify the source of changes in all cases. To mitigate this risk, the STB will implement additional monitoring tools such as Varonis that will close the gap. The STB is also planning to participate in the DHS's CDM program. The CDM program will provide the STB with single-source auditing capability that will expedite the change detection process.

The STB has specified roles and responsibilities for each member of the IT team, but because of the small number of staff, implementing separation of duties has been challenging. The STB has made some progress in this area, but full implementation of separation of duties remains a goal.

Leadership | Currently, senior leadership plays an oversight role in the implementation of the STB's cybersecurity risk management strategy. The IT Security team meets, at a minimum, weekly with the Senior Accountable Official (SAO) to brief ongoing security activities and, as necessary, to provide a summary of potential risks and threats that may impact the STB. The SAO meets with other senior leadership biweekly and provides relevant IT security program updates during those meetings. If questions are raised about IT security during the senior leadership meetings, the Information Systems Security Manager (ISSM) will provide clarification and additional information. Additionally, the CIO and ISSM work together daily to coordinate and improve the STB's IT security program and capabilities.

Senior leadership is also actively engaged in IT security related procurement decisions and all major procurement decisions are approved by the head of the agency. The SAO, with input from the ISSM, makes procurement recommendations to the head of the agency based on gaps identified in the IT security strategy.

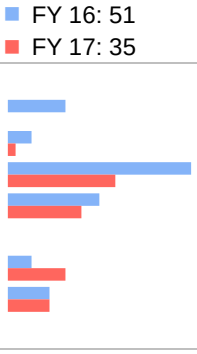
Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. STB became an independent agency in December 2015. Until then, STB was part of the Department of Transportation (DOT) and within the DOT security perimeter. After leaving DOT, STB did not issue any cybersecurity policy and procedures until 15 months later -- after it began the 2017 FISMA audit. However, there were areas that were not covered by these policies and procedures. For example, Information Security Continuous Monitoring did not have any formal policies or procedures. This contributed heavily into the determination that STB was "AD HOC" in all function areas. Because STB's cybersecurity program is in its infancy, it is still not effective. The next steps for STB will be to complete the gaps in its policies and procedures while implementing or continuing implementation of those that it has completed.

FY 2017 Annual Cybersecurity Risk Management Assessment
Tennessee Valley Authority

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	7	0
External/Removable Media	3	1
Improper Usage	22	13
Loss or Theft of Equipment	11	9
Physical Cause	NA	0
Web	3	7
Other	5	5
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Tennessee Valley Authority (TVA) identified its HVAs and Mission Essential Functions and works to continually evaluate the cybersecurity risks to the agency. TVA manages and tracks cybersecurity risk at the enterprise level and has identified risks that include a cyberattack or exploit resulting in protected information being disclosed, and regulatory compliance violations.

Additionally, TVA is working to track and mitigate operational IT risks that may be contributing to cybersecurity risks. These risks include IT infrastructure asset failure, software asset failure, and physical cable plant degradation and failure. After TVA conducted cybersecurity risk assessments of its HVAs, the agency developed an overall risk profile for these assets. TVA underwent six external programmatic and/or regulatory reviews to assess its cybersecurity posture. These reviews encompassed cybersecurity risks and the management of those risks.

Strategy | Cybersecurity efforts at TVA utilize an enterprise-wide, risk-based approach to identifying and managing risks. Staff evaluate risks on an ongoing basis and specific risk factors including threats, vulnerabilities, likelihoods, impact, and velocity are included in the evaluations. The evaluation results are reviewed by a risk analyst and elevated for a higher-level review if needed. Based on a final risk evaluation, TVA leadership provides a decision on risk acceptance or mitigation strategies, which may include a Plan of Action and Milestones.

Resources | TVAs identified cybersecurity and IT operational risks have specific programs, projects, and action plans developed to close identified gaps based upon the risk criticality and asset prioritization. TVA mission drives these decisions and then budget and resources are aligned to ensure the highest risks are mitigated first.

Leadership | In accordance with OMB Circular A-123, the TVA CIO and CISO meet with the TVA Executive Management Council and the TVA Board of Directors multiple times a year. The CIO and CISO provide cybersecurity risk status updates and annual cybersecurity training to all board members. In addition to these regular updates, the CISO provides quarterly updates on the cybersecurity risk posture and associated remediation gaps to the TVA Board. TVA's cybersecurity efforts are also aligned with our ERM team. Cybersecurity metrics are incorporated in the agency risk scorecard that is then reviewed with internal and external stakeholders.

Cybersecurity program efforts are reviewed on an annual basis with senior leadership as part of the budgetary processes. Using established cybersecurity metrics, progress on initiatives and corresponding budgetary information is communicated to senior leadership on a monthly basis as part of the Financial and Operational Performance reports. These focused reporting efforts allow senior management to evaluate how resources are allocated across the enterprise and has positively affected the rate at which the Cybersecurity Program is maturing.

Inspector General Assessment

Based on the analysis of the metrics and associated maturity levels defined with the FY 2017 IG FISMA metrics, the auditors found TVA's security program was operating in an effective manner. The FY 2017 IG FISMA metrics recommend a majority of the functions be at a maturity level 4, "Managed and Measurable," or higher to be considered effective. TVA had four of the five functions rated at a level 4, "Managed and Measurable."

The auditors recommend the CIO perform a risk assessment of the FY 2017 IG FISMA metrics rated at a level 3 (consistently implemented) and determine actions necessary to reduce cybersecurity risk to the agency in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

United States AbilityOne Commission

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

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The United States AbilityOne Commission (AbilityOne) needs a dedicated team to address policies, procedures documentation shortfalls, and plans for Change Management, Risk Assessment, Threats and Vulnerability Scans, Identification and Remediation, Contingency Planning, Incident Response, Business Continuity and Disaster Recovery. Currently, AbilityOne has no acceptable risks. The agency needs to address known risks to the physical security of equipment, availability of information systems and services, and integrity and confidentiality of data.

Strategy | AbilityOne is considering the transfer of risks related to hardware and services to the cloud.

Resources | AbilityOne requires increased budget resources to address agency risks, including the creation of policies and acquisition of tools. Additionally, the agency needs to define and communicate the IT Department's management processes to the organization so that there is clear understanding of timelines and steps for obtaining IT services.

Leadership | AbilityOne's senior leaders are involved in the development of cybersecurity risk management policies and procedures. The agency plans to review the documents every six months.

Inspector General Assessment

The OIG determined through independent review that the agency does not have an effective information security program. The U.S. AbilityOne Commission continues to make strides with respect to inventory management, and the development of procedures on the technology activities performed. Incidentally, the agency needs to focus in the area of formalized and documented policies, and the strategy for consistent implementation on meeting the security requirements for the information system in its operational environment. Furthermore, the U.S. AbilityOne Commission needs to make specific improvements in the areas of vulnerability scanning, Security Assessment and Authorization (SA&A) package, and Continuous Monitoring; as well as other areas (e.g. training for incident response and contingency planning).

FY 2017 Annual Cybersecurity Risk Management Assessment

United States Access Board

Framework	RMA Rating	IG Rating
Overall	At Risk	
Identify	High Risk	Not Applicable
Protect	At Risk	Not Applicable
Detect	Managing Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The Access Board has completed an Authority to Operate of its IT network. As part of this process, the agency has categorized its information system and data. Its HVAs are hosted with Federal Certified cloud hosted providers.

Strategy | The Access Board is in the process of developing an IT roadmap to include security and risk mitigation requirements. The current ATO Cybersecurity review is the first step in creating governance at the enterprise level that will eventually be incorporated into the NIST Cybersecurity Framework.

The Access Board has mitigated risks by transferring mission essential functions to cloud-hosted services, such as MS Office 365, SharePoint FedRAMP-certified and Azure data storage. In addition, the agency transferred risk to IT support contractors for IT support solutions and records management application by leveraging and inheriting the FedRAMP security controls with the ATOs that those contractors currently have in place. Additionally, we have has transferred and mitigated risk by leveraging the security controls of its human resources, accounting, budget, travel, and acquisition shared service providers.

The Access Board has been working with the DHS's CDM program team for more than three years and is actively awaiting the implementation of the CDM Task Order 2F cloud-based continuous diagnostic monitoring program. As a micro-agency with 30 employees, the agency's risk management strategy includes leveraging shared services and acquisition requirements to manage security risk.

Resources | The Access Board ATO process has identified prioritized risks and security gaps that will be addressed in the ongoing development of the Federal Risk Management Plan. The agency has developed plan of actions and milestones to address gaps and security deficiencies in continuity planning, disaster planning, and incident response planning.

The Access Board is using the Cybersecurity Executive Order to bring the key stakeholders into the conversation to address agency budget gap areas. The ATO review process has identified that the agency's status as a micro agency and chronic lack of financial and staffing resources are the most direct and the most significant risk that impacts the agency's ability to resolve highest-priority risks. Furthermore, years of continuous resolution budgets have prevented any new procurement actions until the second or third quarter of each FY.

Leadership | The Access Board's senior leadership is apprised of security related risk management issues on a monthly basis. A partially-implemented cybersecurity risk management strategy impacts the agency's budget process and financial planning process.

Inspector General Assessment

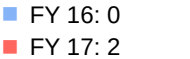
An independent evaluation of the status of the cybersecurity program for United States Access Board was not performed for FY 2017, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an IG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. United States Access Board will explore contracting with an independent assessor in FY 2018.

FY 2017 Annual Cybersecurity Risk Management Assessment

United States African Development Foundation

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	2
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The United States African Development Foundation (USADF) develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy.

Through careful analysis of risk supporting the USADF's business processes and the latest annual security control assessment, the USADF identified the following risks ratings to our HVAs and Mission Essential Functions:

- Low risk: USADF General Support System, USADF Program Support System, messaging and vital records, and Grant Database Management System; and
- Moderate risk: external government shared systems – PRISM (Treasury), Oracle Discoverer (Treasury), payroll (Interior), human resources (Interior), and travel (GSA).

Strategy | USADF implemented a Risk Management Plan that covers risk management of all the Foundation's information resources, whether managed or hosted internally or externally. Information Resources are categorized based on their function, threat exposure, vulnerabilities and data type pursuant to the respective System Security Plan (SSP).

The risk analysis process is updated when environmental, operational, or technical changes arise that impact the confidentiality, integrity, or availability of Information Resources.

The strategies for risk remediation are proportionate to the risks to the Information Resource. The selected and implemented risk management measures reasonably protect the confidentiality, integrity, and availability of Information Resources and the risk is managed on a continuous basis.

Resources | The USADF CISO has identified budget concerns as the largest gap to resolve our highest priority risks that are aligned with efforts and resources needed to close the gaps and mitigate/remediate risk.

Leadership | The results of Risk Analysis and Risk Remediation are documented and reviewed by Senior Managers, the applicable Information Security Officer, System Owners, Data Owners, and IT Custodians. Management processes are used by senior leadership in the development and ongoing implementation of USADF's cybersecurity risk management strategy and processes used to evaluate the effectiveness of security controls.

USADF's CISO ensures active involvement of information system owners and common control providers, CIOs, senior officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Inspector General Assessment

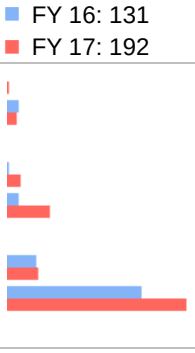
USADF's information security program was evaluated as part of the FY 2017 FISMA Audit. This audit included an evaluation of selected controls from USADF's entire population of seven FISMA reportable systems. The FY 2017 FISMA audit noted 71 of 91 selected NIST SP 800-53, Revision 4 security controls were properly implemented. This led to the determination of USADF having an overall effective information security program. There were a few recommendations made to help USADF improve their information security program. These recommendations can be found in the FY 2017 FISMA audit report.

FY 2017 Annual Cybersecurity Risk Management Assessment

United States Agency for International Development (USAID)

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

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	1
E-mail	8	7
External/Removable Media	0	0
Improper Usage	2	10
Loss or Theft of Equipment	8	30
Physical Cause	NA	0
Web	20	21
Other	93	123
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The United States Agency for International Development (USAID) detects and mitigates more than 200,000 malware and intrusion events per month. USAID recently assessed its cybersecurity program using the NIST Cybersecurity Framework. This assessment revealed important vulnerabilities and, in response, USAID developed and is implementing a plan to achieve improved cybersecurity by the end of FY 2019; however, USAID requires additional financial and human resources to achieve this goal.

USAID also recently underwent a DHS cybersecurity assessment of its HVAs that identified some security risks, and is working to address these gaps.

Strategy | USAID's OCIO has been actively addressing all identified risks from recent DHS assessments on an ongoing basis. A tiger team is taking an agile approach to fixing all vulnerabilities as they are identified, applying patches, updating permissions and implementing new tools. This will be an ongoing process as the risk profile continues to evolve in today's fast-moving cyber environment.

OCIO developed a FISMA Roadmap to address the identified gaps in NIST Cybersecurity Framework implementation. The Roadmap prioritizes where to commit based on risk severity, likelihood of occurrence, and potential significance of impact. For example, USAID is implementing Security Information and Event Management and procuring an Identity and Access Management program to address the Protect function requirements.

Resources | USAID identified the gaps below and corresponding mitigation plans to address high-priority risks. USAID will require additional funding to put the following initiatives in place, along with the authority to hire trained cybersecurity and privacy staff with the appropriate skills sets:

- Lack of an ERM strategy. USAID has an ERM Team that has developed a set of recommendations that include defining the agency's risk appetite and risk tolerance levels and establishing an ERM roadmap and strategy, comprised of ERM governance (e.g., Risk Management Board), artifacts (e.g., risk registers), ERM metrics, and an ERM Dashboard;
- A more strategic approach to Information Security Continuous Monitoring, including the use of a Security and Information Event Management for security analysis and risk management;
- A more mature Enterprise Security Operations Center (ESOC), with interoperable tools and higher staffing levels. USAID is currently researching vendor ESOC options to enhance its incident response, metrics and measurements, and risk management capabilities; and
- A more consistent implementation and testing of recovery and continuity plans at all organizational levels.

Leadership | USAID appraises the Assistant Administrator for Management (AA/M), of risks within the enterprise through weekly meetings and daily communication with the CIO. In addition, USAID follows emergency procedures whereby risks of an immediate nature are briefed to senior leadership on an as-needed or emergency basis.

USAID's cybersecurity risk management strategy integrates with the broader ERM process required by OMB's Circulars A-123 and A-130. USAID plans to institute an ERM governance structure, leveraging existing offices or functions within the organization that currently monitor risks, such as OCIO's Security Assessment and Authorization (SA&A) process, the agency's Management Control and Review Committee (MCRC), and the establishment of a Chief Risk Officer. When complete, this process will specifically integrate cybersecurity risk and agency-wide enterprise risk to appropriately categorize these risks according to their likelihood and impact and briefed to agency leadership.

Inspector General Assessment

Although progress is needed to move to the next maturity level (Level 4, Managed and Measurable), we determined the USAID's overall information security program was effective based on the FY 2017 IG FISMA Reporting Metrics results and the results of the agency's FY 2017 FISMA Audit. The audit included an evaluation of six information systems at USAID and noted that 150 of the 162 selected NIST SP 800-53, Revision 4 security controls were properly implemented. To address weaknesses identified, the audit recommended that USAID:

- Track and remediate persistent vulnerabilities.
- Configure vulnerability assessment tools to detect vulnerabilities previously undiscovered by internal scans.
- Migrate unsupported applications from their existing platform to vendor-supported platforms.
- Annually assess risks for all internal and external systems in accordance with agency policy.
- Require system owners to verify their procedures for revoking system access accounts for separated and transferred employees and contractors are enforced.
- Review and analyze remote access connections.

FY 2017 Annual Cybersecurity Risk Management Assessment

United States Trade and Development Agency

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	High Risk	Defined
Recover	Managing Risk	Managed and Measurable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The U.S. Trade and Development Agency (USTDA) has identified numerous risks in its cybersecurity posture. USTDA utilizes the NIST SP 800-53 for its assessment and authorization processes; USTDA is completing their update. Additionally, USTDA utilizes CDM tools, which are currently not fully integrated with enterprise tools. USTDA plans to reduce these risks by transferring risk and implementing enhanced automation via the HDS CDM program when the agency moves to its new facility next year.

USTDA utilizes Department of State (State) for its shared service provider; however, State has not yet setup PIV cards for logical authentication for the agency. The agency is mitigating this risk by using RSA two-factor authentication tokens. The agency is working with State and the GSA to finalize the PIV implementation process.

A certain portion of the agency's mission services do not have higher levels of robustness and resilience. USTDA plans on transferring its group network shared drives and SharePoint services to the cloud in FY 2018 to mitigate this risk.

Strategy | The agency utilizes the NIST Cybersecurity Framework to evaluate its cybersecurity posture. These risk management recommendations and categorizations are prepared weekly by the CIO, Senior Accountable Official for Risk Management, and discussed with the Agency Head and Deputy Agency Head. In addition, capital acquisitions and decisions have the NIST Cybersecurity Framework embedded into them.

Resources | The agency identified deployment of CDM capabilities at the enterprise level, TIC implementation, PIV card logical access, and updating the agency's A&A as priorities. Enterprise-wide CDM and TIC implementation are aligned with the agency's upcoming physical relocation next year. The agency is looking to create an integrated product team between USTDA, State, and GSA next year.

Leadership | Enterprise-level risk management recommendations and categorizations are prepared weekly by the CIO, who is the Senior Accountable Official for Risk Management, and discussed with the Agency Director and Deputy Agency Director. In addition, capital acquisitions and major decisions have mission impacts built into them. The impact of this high level of engagement among senior leadership is that everyone has a synchronized understanding of enterprise risks, and is in agreement on resource allocation, and as a result allocation is efficient.

Inspector General Assessment

An independent external audit determined that USTDA has an effective information security program. The USTDA security program continues to be incorporated into its annual performance and security plans in accordance with the law, providing reasonable assurance and safeguards to maintain integrity, and competence.

FY 2017 Annual Cybersecurity Risk Management Assessment

Vietnam Education Foundation

Framework	RMA Rating	IG Rating
Overall	High Risk	
Identify	High Risk	Not Applicable
Protect	High Risk	Not Applicable
Detect	At Risk	Not Applicable
Respond	High Risk	Not Applicable
Recover	High Risk	Not Applicable

FY 16: 0
FY 17: 0

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	0	0
External/Removable Media	0	0
Improper Usage	0	0
Loss or Theft of Equipment	0	0
Physical Cause	NA	0
Web	0	0
Other	0	0
Multiple Attack Vectors	0	0

CIO Risk Management Self-Assessment

Risks | The largest cybersecurity threat is to Vietnam Education Foundation's (VEF) Online Management System (OMS), which is a database accessible to VEF staff that houses most of the agency's sensitive information. The OMS is an important part of the agency's operations and would have a significant impact on overall agency operations if rendered inoperable. Additionally, as a small agency with only four staff, VEF does not have a server and VEF employees use laptops that are password protected.

Strategy | VEF has contracted with several firms to help the agency meet FISMA requirements and protect its information systems. The agency has taken special steps to protect its OMS from cybersecurity attacks. In 2016, VEF moved the OMS to a more secure server location and the agency is in the final phases of making the most sensitive sections of the OMS accessible only using PIV cards. The agency will sunset in 2018, and continues to work with its contractors to protect its information systems while it prepares for its permanent closure.

Resources | The firms contracted to protect the agency's information systems provide regular input on the highest-priority risks to address. VEF will continue funding at the current level to protect its information systems while making preparations for its permanent closure in 2018. The agency continues to work toward protecting its highest-value assets, namely OMS, through the implementation of PIV cards and ongoing maintenance and monitoring of the server on which it operates.

Leadership | Our senior leadership plays an important role in meeting the potential cybersecurity threats facing the agency. The leadership reviews the actions taken by VEF contractors on a monthly basis, and the contractors provide input on any emerging security threats. VEF continues to work toward FISMA compliance with its contractors. Leadership focused agency efforts to improve the security of the OMS, as they understand that an attack could have a significant impact on its programming and operations. Given VEF's imminent closure in 2018, the agency's focus will be on protecting its data while it prepares to close down all of its systems.

Inspector General Assessment

An independent evaluation of the status of the IT cybersecurity program for Vietnam Education Foundation was not performed for FY 2017, 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. Vietnam Education Foundation will explore contracting with an independent assessor in FY 2018.

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
OCIO – 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