



# **Federal Information Security Modernization Act of 2014**

**Annual Report to Congress**

**Fiscal Year 2016**

*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). 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 2016 data reported by agencies to OMB and DHS on or before November 13, 2016.*

# Table of Contents

Executive Summary: The State of Federal Cybersecurity .....	3
Section I: Federal Cybersecurity at a Glance .....	4
A. Federal Cybersecurity Roles and Responsibilities .....	4
B. Government-wide Cybersecurity Programs .....	5
C. Initiatives to Enhance Federal Cybersecurity Oversight.....	7
D. FY 2016 Policy Updates .....	9
Section II: FY 2016 Agency Performance .....	11
A. Federal Cybersecurity Roles and Responsibilities .....	11
B. Agency Cybersecurity Performance Summaries .....	18
C. FY 2016 Major Information Security Incidents .....	111
Section III: Enhancing Privacy Programs .....	113
A. Progress in Meeting Key Privacy Performance Measures .....	113
B. Information Systems – Privacy Impact Assessments.....	113
C. Information Systems – System of Records Notices .....	114
D. Privacy Training and Accountability .....	114
Section IV: Appendices .....	116
Appendix 1: IT Security Spending Reported by CFO Act Agencies.....	116
Appendix 2: Acronyms and Abbreviations .....	117

# Executive Summary:

## The State of Federal Cybersecurity

In 2016, cybersecurity continued to become a household term among the American public, as millions of citizens had their personal data and devices exposed to ever-expanding cyber threats. During the year, malicious actors compromised several social media and email services, leading to the exposure of personal data for a large portion of their user bases. In October 2016, a distributed denial of service attack used seemingly innocuous internet-connected devices to cripple servers that connect the public to many popular websites. The exploits that led to these cyber incidents were not new, and demonstrate that we must redouble our efforts to inform Americans and companies across the country of methods that they can employ to protect their data from malicious actors.

Federal agencies were not immune to these exploits in 2016, with over 30,899 cyber incidents that led to the compromise of information or system functionality. Sixteen of these incidents met the threshold for a major incident, a designation that triggers a series of mandatory steps for agencies, including reporting certain information to Congress.

During the year, Federal agencies made considerable progress in strengthening their defenses and enhancing their workforces to combat cyber threats. In particular, agencies worked to enforce the use of multi-factor Personal Identity Verification (PIV) cards, with 81% of government users now using this credential to access Federal networks. Additionally, over 70% of Federal agencies have employed strong anti-phishing and malware capabilities to help safeguard their networks from malicious activity. Agencies have also made significant progress toward safeguarding their high value information technology (IT) assets and employing capabilities to identify, detect, and protect hardware and software assets on their networks.

The Office of Management and Budget (OMB) worked with agencies to develop policies aimed at strengthening cybersecurity across the government, including a revision to [OMB Circular A-130, Managing Information as a Strategic Resource](#), which sets the overarching framework for managing Federal IT resources. OMB also collaborated with the Office of Personnel Management (OPM) to publish the first-ever [Federal Cybersecurity Workforce Strategy](#) to help agencies recruit and retain top cyber talent. OMB and its interagency partners look to build on these policies and continue driving cybersecurity performance in the coming years.

This annual report provides Congress with information on agencies' progress towards meeting cybersecurity performance goals in Fiscal Year (FY) 2016 and the results of the independent Inspectors General (IGs) assessments that identify areas in need of improvement. This report also provides information on Federal cybersecurity incidents, ongoing efforts to mitigate and prevent future incidents, and agencies' progress in implementing cybersecurity policies and programs to protect their systems, networks, and data.

# Section I: Federal Cybersecurity at a Glance

## A. Federal Cybersecurity Roles and Responsibilities

Securing Federal data, IT systems, and networks is the shared responsibility of all government agencies. 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):** In accordance with the [Federal Information Security Modernization Act of 2014](#) (FISMA), OMB is responsible for overseeing Federal agencies' information security practices and developing and implementing related policies and guidelines. The Federal Chief Information Security Officer (CISO) leads the OMB Cyber and National Security Unit (OMB Cyber), which serves as the dedicated team within the Office of the Federal Chief Information Officer that works with Federal agency leadership to address information security priorities. OMB Cyber 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.

**National Security Council (NSC):** The NSC is the Executive Office of the President component responsible for coordinating 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):** FISMA designates DHS as the operational lead for Federal cybersecurity and provides DHS authority to coordinate government-wide cybersecurity efforts, issue binding operational directives to agencies on actions 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 ) and [Continuous Diagnostics and Mitigation](#) (CDM) program, conducts risk assessments, and provides incident response assistance 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 Highly Adaptive Cybersecurity Services (HACS), which GSA designed to provide agencies with quick, reliable access to key services before, during, and after cyber-related incidents occur.

## Section I: Federal Cybersecurity at a Glance

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 a technically oriented agency 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 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.

**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 are responsible for the security of Federal information and information systems. 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 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.

### B. Government-wide Cybersecurity Programs

Although each agency is ultimately accountable and responsible for its cybersecurity, DHS and GSA manage a series of government-wide programs that provide agencies with consistent, cost-effective solutions to help secure Federal systems and information.

#### **Continuous Diagnostics and Mitigation (CDM)<sup>1</sup>**

The DHS CDM program provides commercial off-the-shelf tools and services that enable Federal, state, local, regional, and tribal governments to strengthen the security posture of their IT networks.

## Section I: Federal Cybersecurity at a Glance

[OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems](#), first described the DHS CDM program. The CDM program installs capabilities on government IT assets to automate select functions of system management, including, but not limited to asset detection, configuration management and vulnerability management. CDM bolsters agencies' ability to identify, prioritize, and mitigate cybersecurity risks on an ongoing basis by automating these management and monitoring capabilities. In addition, agencies may analyze data from these sensors to enhance their processes for managing the assets, users and data on their networks.

### **National Cybersecurity Protection System (EINSTEIN)**

The National Cybersecurity Protection System (which includes EINSTEIN) provides the Federal Government with improved situational awareness of intrusion threats to Federal Executive Branch civilian networks through near real-time identification and prevention of malicious cyber activity. Following widespread deployment of EINSTEIN 2, a passive intrusion detection system that issues alerts when it detects threats, DHS began deploying EINSTEIN 3 Accelerated (E<sup>3</sup>A) in 2012. E<sup>3</sup>A provides agencies with an intrusion prevention capability that can block and disable attempted intrusions before they can cause harm. By contracting with major Internet Service Providers, the initial deployment of E<sup>3</sup>A focused on countermeasures that address approximately 85% of the cybersecurity threats affecting Federal civilian networks. Additionally, DHS has introduced an E<sup>3</sup>A Service Extension to provide similar countermeasures for those agencies with Internet Service Providers that do not offer E<sup>3</sup>A protections. The implementation of EINSTEIN capabilities, along with tools provided under CDM, are foundational to the Defense-in-Depth approach set forth in the DHS Intrusion Assessment Plan. As of the end of FY 2016, DHS had deployed E<sup>3</sup>A to protect 93% of all Federal users.

### **Federal Risk and Authorization Management Program (FedRAMP)**

GSA administers FedRAMP, which is a government-wide program that applies a standardized approach to validate that cloud products and services meet Federal cybersecurity standards. The CIOs from DOD, DHS, and GSA make up the Joint Authorization Board, which serves as the governance and decision-making body for FedRAMP. The program increases confidence in the validity of cloud security claims, promoting consistency in security authorizations by using a baseline set of agreed-upon standards. This approach ultimately avoids redundancy, costs, and other inefficiencies that can emerge with traditional methods of IT system management. Additionally, FedRAMP offers multiple paths to allow cloud service providers to certify their products once and leverage the certification to sell their products and services to multiple agencies.

### **Highly Adaptive Cybersecurity Services (HACS)**

In support of the [Cybersecurity National Action Plan](#), GSA added four HACS to IT Schedule 70, the Federal Government's primary IT acquisition vehicle, to provide agencies quick, reliable access to key services before, during, and after cyber-related

## Section I: Federal Cybersecurity at a Glance

incidents. These HACS provide interested agencies with the opportunity to purchase advanced security testing tools and capabilities similar to those provided by the DHS National Cybersecurity Assessment and Technical Services team, which provides scheduled assessments to agencies. Services include:

- Penetration testing;
- Incident response;
- Cyber hunt; and
- Risk and Vulnerability Assessments.

Vendors undergo rigorous evaluation based on criteria established by GSA and DHS. GSA projects that utilizing the Schedule 70 HACS will allow agencies to obtain services 25%-50% more quickly than if they had ordered on the open market.<sup>2</sup>

### C. Initiatives to Enhance Federal Cybersecurity Oversight

The subsections below detail FY 2016 initiatives to oversee and improve Federal agencies' cybersecurity performance and address known cybersecurity gaps.

#### Cybersecurity National Action Plan

The Cybersecurity National Action Plan built on lessons learned from cybersecurity trends, threats, and intrusions. The Cybersecurity National Action Plan included a series of actions to increase the level of cybersecurity dramatically in both the Federal Government and the Nation's larger digital ecosystem as a whole. Key activities included:

- Creating the Federal CISO position to modernize and transform how the government manages cybersecurity.
- Releasing [OMB Memorandum M-16-15, Federal Cybersecurity Workforce Strategy](#), which details government-wide actions to identify, recruit, and retain a highly-capable workforce to address complex and ever-evolving cyber threats.
- Establishing the Commission on Enhancing Cybersecurity made up of top thought leaders from outside government. The Commission issued their [Report on Securing and Growing the Digital Economy](#) in December 2016 and recommended actions to strengthen cybersecurity in both the public and private sectors over the next decade.

#### OMB's Oversight of Agency Performance

OMB Cyber expanded its interaction with Federal agencies and its oversight of their cybersecurity programs through FY 2016. In particular, OMB Cyber expanded the use of CyberStat Reviews, which are engagements with agency leadership to accelerate progress toward achieving FISMA performance goals.<sup>3</sup> OMB, in close coordination with



## Section I: Federal Cybersecurity at a Glance

DHS, expanded the program from 14 reviews in FY 2015 to 24 reviews in FY 2016. OMB and DHS work with agencies to develop action items that address risks through these reviews, identify areas for targeted assistance, and track performance throughout the year.

These reviews have led to improvements at individual agencies and across the Federal Government. FY 2016 accomplishments included:

- Ensuring that agencies continue to identify, prioritize, and protect systems that are of particular interest to potential adversaries, and encouraging agencies to partner with DHS to conduct Risk and Vulnerability Assessments of high value assets and address security gaps.
- Identifying challenges that have prevented some agencies from enforcing the use of PIV cards for all network users and connecting those agencies with subject matter experts to overcome specific technical and policy challenges.
- Engaging with agency CIOs on governance challenges and sharing best practices for using department-level strategies, assessments, and scorecards to inform leadership of cybersecurity priorities and track agency performance against set goals.
- Ensuring that agencies have robust Information Security Continuous Monitoring (ISCM) programs to support the implementation of asset, configuration, and vulnerability management tools as part of the capabilities provided under the DHS CDM program.

In addition to these comprehensive, deep-dive reviews, OMB conducts frequent engagements to promote agency implementation of necessary information security measures. OMB generally holds these meetings with the agency CISOs or Information Security Senior Officials, and leverages agency-reported FISMA metrics to understand reasons for lagging performance. These engagements inform future CyberStat Reviews and aid OMB in streamlining its oversight processes.

Additionally, OMB reviews data from the 23 civilian CFO Act agencies on a quarterly basis as part of the President's Management Council Cybersecurity Assessment, which reviews agency programs against government-wide cybersecurity performance goals. In the first quarter of FY 2016, only five of these agencies had information security programs that met or exceeded government-wide performance goals. By the end of FY 2016, 13 agencies had met these goals and all others were making significant progress toward this end as a direct result of the oversight mechanisms described above.

# Section I: Federal Cybersecurity at a Glance

## D. FY 2016 Policy Updates

### OMB Circular A-130

[OMB Circular No. A-130, Managing Information as a Strategic Resource](#), is the government's overarching policy for managing Federal information resources. FISMA required OMB to update this foundational policy, and OMB collaborated with interagency partners to update Circular A-130. The revised Circular A-130 provides a wide range of policy updates for Federal agencies regarding cybersecurity, information governance, privacy, records management, open data, and acquisitions. It also establishes a general policy for IT planning and budgeting through governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Circular A-130 directs Federal agencies to consider information security and privacy as a more dynamic, comprehensive, strategic, and risk-based program. Agency CIOs and IGs are already incorporating the elements of the revised Circular into the program management and program assessment processes.

### Federal Cybersecurity Workforce Strategy

Both government and private industry face a persistent shortage of cybersecurity and IT talent to implement and oversee information security protections to combat cyber threats. OMB and OPM worked with workforce experts across the government to develop [OMB Memorandum M-16-15, Federal Cybersecurity Workforce Strategy](#). The Workforce Strategy seeks to enhance the government's ability to identify, recruit, develop, and retain talent while expanding the workforce pipeline of the best and brightest individuals in cybersecurity. Specifically, the policy calls for expanding cybersecurity education and training, new efforts to recruit top cyber talent, improving development and retention programs and incentives, and enhancing efforts to identify and close shortages that exist in the cybersecurity workforce. Agencies are already making considerable progress toward addressing workforce shortages, as they hired over 7,500 cybersecurity and IT employees in 2016; by comparison, Federal agencies hired 5,100 cybersecurity and IT employees in 2015.

### Cyber Incident Coordination

As the threat of the compromise of essential IT resources has increased across sectors, so has the need for a clearly articulated plan for the coordination of Federal response activities. [Presidential Policy Directive](#) (PPD-41) serves this function, setting forth principles and processes to guide the government's response to information security incidents in both the public and private sectors. PPD-41 clearly articulates incident response processes and outlines the responsibilities of key agencies and entities across the government, including OMB, DHS, NSC, FBI, and the Intelligence Community. PPD-41 promotes a well-coordinated response that brings to bear the capabilities of the Federal Government to mitigate the damage of cybersecurity incidents and enable the restoration and recovery of affected systems.

# Section I: Federal Cybersecurity at a Glance

## High Value Assets (HVAs)

OMB required agencies to identify and safeguard HVAs during the 2015 Cybersecurity Sprint and the ensuing [OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan](#). HVAs are the assets, Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. In early FY 2017, OMB emphasized the value 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](#). Specifically, all agencies will continuously review all critical assets, systems, information, and data in order to understand the potential impact of a cyber incident on those assets and ensure robust physical and cybersecurity protections are in place.

## Section II: FY 2016 Agency Performance

### A. Federal Cybersecurity Roles and Responsibilities

OMB worked with agency CIOs and IGs throughout FY 2016 to provide the Annual FISMA Report readers with context around individual agencies' performance. Previous FISMA reports provided a high-level overview of Federal cybersecurity performance, but did not provide narrative context around agencies' progress and constraints. This year's Annual 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." These narratives contain four sections: CIO Assessment, IG Assessment, Cross-Agency Priority (CAP) Goal Metrics, and U.S. Computer Emergency Readiness Team (US-CERT) Incidents.

The following provides a description and a summary of each section:

#### **Chief Information Officer Assessment**

OMB collects annual performance metrics from agency CIOs in which agencies are required to detail progress and challenges across their respective information security programs. The CIO metrics apply criteria from OMB guidance and NIST standards and are OMB's primary method for tracking agencies' performance against those standards. 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.

#### **Cybersecurity CAP Goal Metrics**

In accordance with the [Government Performance and Results Modernization Act of 2010](#),<sup>4</sup> CAP Goals offer a mechanism for accelerating progress in priority areas in which implementation requires active collaboration between OMB and Federal agencies. The Cybersecurity CAP goal has already improved awareness of security practices, vulnerabilities, and threats to the operating environment by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity. Agencies report progress toward this goal as part of the [FISMA CIO Metrics](#), which apply criteria from NIST standards and guidance to cybersecurity performance metrics. The CAP goal metrics provide a method for tracking agencies' compliance with, and application of NIST standards and guidance to their enterprise. OMB publishes the CFO Act agencies' results in quarterly cybersecurity CAP Goal reports, along with other CAP Goal reports, on [performance.gov](#). Agency performance on the Cybersecurity CAP goal also informs many of OMB's oversight activities. Eighty-nine (89) agencies submitted FISMA metrics in 2016, 23 CFO Act Agencies and 66 Small Agencies.

The FY 2015-FY 2017 Cybersecurity CAP goal has three priority areas:

# Section II: FY 2016 Agency Performance

1. **Information Security Continuous Monitoring Mitigation (ISCM).** The goal of ISCM is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization’s cybersecurity posture, hygiene, and operational readiness. The ISCM CAP goal has four performance areas: Hardware Asset Management,<sup>5</sup> Software Asset Management,<sup>6</sup> Vulnerability Management,<sup>7</sup> and Secure Configuration Management.<sup>8</sup> Each area has a target performance of 95% for all capabilities. [CDM Phase 1](#) will assist agencies in establishing these ISCM capabilities and provide greater visibility as to the assets on each agency’s network.

Table 1 provides summary data for these metrics based on data from a total of 89 agencies.

**Table 1: FY 2015 and FY 2016 ISCM Summary**

CAP Goal Metric	Metric Target	Number of Agencies Meeting Target	Implementation Percentage Across all Agencies*	■ 2015 ■ 2016
Hardware Asset Management	95%	35	61%	
		32	61%	
Software Asset Management	95%	21	54%	
		35	61%	
Vulnerability Management	95%	28	70%	
		60	90%	
Secure Configuration Management	95%	39	91%	
		62	92%	

\*The percentages in this table are calculations of the number of compliant assets across the government/ total number of assets across the government. Analysis of FISMA Agency Level Questions Data (Questions 1.2, 1.4, 1.5, 2.2, 2.3, 3.16, 3.17), reported to DHS via CyberScope from October 1, 2015, to September 30, 2016. OMB used a weighted average of the total number of applicable assets to determine the government-wide average.







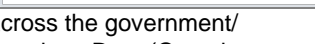
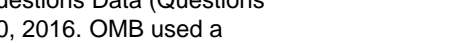
2. **Identity, Credential, and Access Management (ICAM).** The goal of ICAM is to implement a set of capabilities that ensure network users use strong authentication to access Federal IT resources and to limit users’ access to the resources and data required for their job functions. This CAP goal area should serve as part of agencies’ broader ICAM program, which consists of identity proofing solutions, physical access, and logical network access controls, among other capabilities. Mature ICAM programs enable agencies to monitor users’ access and implement secure capabilities such as single sign-on, which provide trusted users with efficient access

## Section II: FY 2016 Agency Performance

to applications and data. The ICAM CAP goal consists of PIV enforcement targets for privileged users (100%) and unprivileged users (85%).<sup>9</sup>

Table 2 provides summary data for these metrics based on data from a total of 89 agencies.

**Table 2: FY 2015 and 2016 ICAM Summary**

<b>CAP Goal Metric</b>	<b>Metric Target</b>	<b>Number of Agencies Meeting Target</b>	<b>Implementation Percentage Across all Agencies*</b>	<b>2015</b>	<b>2016</b>
Unprivileged User PIV Implementation	85%	27	62%		
		40	81%		
Privileged User PIV Implementation	100%	24	78%		
		40	89%		







\*The percentages in this table 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 (Questions 2.4, 2.5), reported to DHS via CyberScope from October 1, 2015, to September 30, 2016. OMB used a weighted average of the total number of applicable users to determine the government-wide average.

- Anti-Phishing and Malware Defense.** The goal of Anti-Phishing and Malware Defense is to implement technologies, processes, and training that reduce the risk of compromise through email and malicious or compromised web sites. These technologies provide agencies with visibility of their network traffic and ensure they can detect, monitor, limit, and/or block malicious traffic, to include encrypted traffic, to and from agency assets. There are three performance areas for this CAP goal, each of which requires agencies to implement a certain number of capabilities across 90% of their infrastructure: Anti-Phishing (agencies must meet five of seven capabilities), Malware Defense (agencies must meet three of five capabilities), and Other Defenses (agencies must meet two of four capabilities).

Table 3 provides summary data for these metrics based on data from a total of 89 agencies.

# Section II: FY 2016 Agency Performance

**Table 3: FY 2015 and FY 2016 Anti-Phishing and Malware Defense Summary**

CAP Goal Metric	Metric Target	Number of Agencies Meeting Target*	2015	2016
Anti-Phishing Defenses	5 of 7	29		
		69		
Malware Defenses	3 of 5	33		
		65		
Other Defenses	2 of 4	51		
		77		

\*Analysis of FISMA Agency Level Questions Data (Questions 2.19, 3.1-3.15), reported to DHS via CyberScope from October 1, 2015, to September 30, 2016.

### Inspector General Assessment<sup>10</sup>

FISMA requires each agency to conduct an annual independent assessment of its information security program and practices to determine their effectiveness. Agencies with an IG must have the IG perform this review, and those without an IG are required to obtain the services of an IG or independent auditor.

In FY 2016, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) IT Committee collaborated with OMB and DHS to align the IG metrics with the five function areas in the [NIST Framework for Improving Critical Infrastructure Cybersecurity](#) (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. This alignment helps promote consistent and comparable metrics and criteria in the CIO and IG metrics processes and, therefore, provides agencies with a meaningful independent assessment of their information security programs.

The IGs began developing maturity models in FY 2015 to provide an in-depth assessment of agency programs in specific areas, beginning with ISCM. In FY 2016, the IGs aligned the ISCM maturity model to the Detect function in the Cybersecurity Framework and added a maturity model for incident response in the Respond function area. The IG community leveraged metrics that align to “maturity model indicators” to assess agency programs in FY 2016, and the CIGIE plans to develop maturity models for the Identify, Protect, and Recover functions in FY 2017. Table 4 details the five maturity levels within each of the five Cybersecurity Framework function areas: Identify, Protect, Detect, Respond, and Recover.

## Section II: FY 2016 Agency Performance

**Table 4: IG Assessment Maturity Levels**

<b>Maturity Level</b>	<b>Maturity Level Distribution</b>	<b>Rating Description</b>
<b>Level 1:</b> Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.	Has not met all metrics designated "Defined"
<b>Level 2:</b> Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.	Met all metrics designated "Defined"
<b>Level 3:</b> Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.	Met all metrics designated "Consistently Implemented"
<b>Level 4:</b> Managed and Measureable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organizations and used to assess them and make necessary changes.	For Identify, Protect, and Recover functions: met half or greater of the metrics designated "Managed and Measureable"  For Detect and Respond Maturity Models: Met all metrics in the "Managed and Measurable" section
<b>Level 5:</b> Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.	For Identify, Protect, and Recover functions: Met all metrics designated "Managed and Measureable"  For Detect and Respond Maturity Models: Met all metrics in the "Optimized" section

This year's independent assessments include maturity model ratings and narrative context for the ratings. In some instances, IGs provided recommendations for addressing performance challenges. This improves upon the format from prior FISMA reports, which simply provided a high-level agency score without providing sufficient context as to what they meant. The narrative section allows IGs and independent third-party assessors to appropriately frame their analysis and offer additional insights into the challenges faced by their agencies, including ongoing efforts to remediate them. Going forward, the IGs, OMB, and DHS will continue to work together to further refine the independent assessment process and provide methodologies for comparing performance across the government. In the interim, Table 5 provides the median maturity model ratings across the five Cybersecurity Framework functions from 75 agency IG and independent assessments.



## Section II: FY 2016 Agency Performance

**Table 5: Median Government-wide Maturity Model Ratings**

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

### US-CERT Incidents by Attack Vector<sup>11</sup>

Agency incident data provides an indication of the threats that agencies endure 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 government and at each Federal agency. The FY 2015 FISMA Report to Congress detailed several limitations of the previous [Federal Incident Reporting Guidelines](#), which led agencies to report on incident types that had no potential impact on operations. For this reason, in FY 2016, US-CERT's revised [Incident Notification Guidelines](#) required agencies to use an incident reporting methodology that classifies incidents by the method of attack, known as attack vector, and to specify the impact to the agency.<sup>12</sup> As such, the FISMA Report captures incidents in accordance with US-CERT's revised guidelines.

The shift to reporting by attack vector means that FY 2016 incident data and prior years' incident data are not comparable. The FY 2016 data does not allow for an apples-to-apples comparison to prior incident data because it focuses on a subset of all malicious attempts to compromise Federal systems that did not exist in the previous reporting guidelines. For this reason, the FY 2016 data does not show a decrease in incidents from prior years, as it is an entirely different way of looking at incidents than prior years.

Additionally, [OMB Memorandum M-17-05, Fiscal Year 2016 – 2017 Guidance on Federal Information Security Privacy Management Requirements](#), requires US-CERT and agencies to conduct quarterly incident reporting validation processes to review and refine incident data. US-CERT initiated an incident reporting data-validation process in late FY 2016, where US-CERT and agencies confirm the number of impactful incidents and improve the overall quality of the incident data for investigative and reporting purposes. This effort helps remove incidents that did not have an impact on an agency such as the non-cyber or scan, probes and attempted access and duplicate incident entries reported by automated systems, such as EINSTEIN, and separately reported by agency employees. These process improvements allowed US-CERT and agencies to

## Section II: FY 2016 Agency Performance

refine the number of impactful incidents to 30,899 incidents across the eight attack vectors detailed in Table 6.

**Table 6: Agency-Reported Incidents by Attack Vector**

<b>Attack Vector</b>	<b>Description</b>	<b>CFO</b>	<b>Non-CFO</b>	<b>Government-wide</b>
Attrition	Employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	108	1	109
E-mail/ Phishing	An attack executed via an email message or attachment.	3,160	132	3,292
External / Removable Media	An attack executed from removable media or a peripheral device.	132	6	138
Impersonation / Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	60	4	64
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	3,920	210	4,130
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	5,313	377	5,690
Web	An attack executed from a website or web-based application.	4,766	102	4,868
Other	An attack method does not fit into any other vector or the cause of attack is unidentified.	11,365	437	11,802
Multiple Attack Vectors	An attack that uses two or more of the above vectors in combination.	789	17	806
<b>Total</b>		<b>29,613</b>	<b>1,286</b>	<b>30,899</b>

OMB and DHS plan to continue leveraging the attack vector schema to allow for trending of incidents' impact to agencies in the coming years.

## Section II: FY 2016 Agency Performance

### B. Agency Cybersecurity Performance Summaries

African Development Foundation .....	21
American Battle Monuments Commission.....	22
Armed Forces Retirement Home.....	23
Barry Goldwater Scholarship and Excellence in Education Foundation .....	24
Board of Governors of the Federal Reserve.....	25
Broadcasting Board of Governors .....	26
Chemical Safety Board.....	27
Commission of Fine Arts .....	28
Commission on Civil Rights.....	29
Committee for Purchase from People Who Are Blind or Severely Disabled.....	30
Commodity Futures Trading Commission .....	31
Consumer Financial Protection Bureau.....	32
Consumer Product Safety Commission.....	33
Corporation for National and Community Service .....	34
Council of the Inspectors General on Integrity and Efficiency .....	35
Court Services and Offender Supervision Agency .....	36
Defense Nuclear Facilities Safety Board.....	37
Denali Commission .....	38
Department of Agriculture .....	39
Department of Commerce .....	40
Department of Defense .....	41
Department of Education.....	42
Department of Energy .....	43
Department of Health and Human Services .....	44
Department of Homeland Security .....	45
Department of Housing and Urban Development.....	46
Department of Justice .....	47
Department of Labor .....	48
Department of State .....	49
Department of the Interior .....	50
Department of the Treasury .....	51
Department of Transportation .....	52

## Section II: FY 2016 Agency Performance

Department of Veterans Affairs .....	53
Election Assistance Commission .....	54
Environmental Protection Agency .....	55
Equal Employment Opportunity Commission .....	56
Export-Import Bank of the United States .....	57
Farm Credit Administration.....	58
Federal Communications Commission.....	59
Federal Deposit Insurance Corporation.....	60
Federal Election Commission.....	61
Federal Energy Regulatory Commission.....	62
Federal Housing Finance Agency .....	63
Federal Labor Relations Authority .....	64
Federal Maritime Commission.....	65
Federal Mediation and Conciliation Service .....	66
Federal Retirement Thrift Investment Board .....	67
Federal Trade Commission .....	68
General Services Administration .....	69
Institute of Museum and Library Services .....	70
Inter-American Foundation.....	71
International Boundary and Water Commission .....	72
International Trade Commission .....	73
Marine Mammal Commission.....	74
Merit Systems Protection Board.....	75
Millennium Challenge Corporation .....	76
Morris K. Udall Foundation.....	77
National Aeronautics and Space Administration .....	78
National Archives and Records Administration .....	79
National Capital Planning Commission .....	80
National Credit Union Administration.....	81
National Endowment for the Arts.....	82
National Endowment for the Humanities .....	83
National Labor Relations Board .....	84
National Mediation Board.....	85

## Section II: FY 2016 Agency Performance

National Science Foundation .....	86
National Transportation Safety Board .....	87
Nuclear Regulatory Commission .....	88
Nuclear Waste Technical Review Board .....	89
Occupational Safety and Health Review Commission.....	90
Office of Government Ethics .....	91
Office of Navajo and Hopi Indian Relocation.....	92
Office of Personnel Management.....	93
Office of Special Counsel.....	94
Overseas Private Investment Corporation.....	95
Peace Corps .....	96
Pension Benefit Guaranty Corporation.....	97
Postal Regulatory Commission .....	98
Privacy and Civil Liberties Oversight Board .....	99
Railroad Retirement Board.....	100
Securities and Exchange Commission .....	101
Selective Service System.....	102
Small Business Administration .....	103
Smithsonian Institution .....	104
Social Security Administration.....	105
Surface Transportation Board .....	106
Tennessee Valley Authority.....	107
United States Access Board.....	108
United States Agency for International Development.....	109
Vietnam Education Foundation .....	110



# Cybersecurity Performance Summary

African Development Foundation

## Chief Information Officer Assessment

The United States African Development Foundation (USADF) has established an information security program that aligns with Federal regulations and includes critical elements such as periodic risk assessments and a complete program evaluation every three years as mandated by the FISMA. USADF has made efforts to document an organization-wide security program, establish a security management structure, ensure that elements of a security program such as asset inventory management, incident and vulnerability management, configuration management, anti-virus/malware/phishing, security and privacy awareness training are implemented, and perform a continuous monitoring program. USADF participates in the DHS Continuous Diagnostics and Mitigation (CDM) Program, and in FY 2016, USADF signed a Memorandum of Agreement (with the DHS to begin implementing the EINSTEIN 3 Accelerated (E<sup>3</sup>A) Managed Trusted Internet Protocol Services. Consistent with the “Cloud First” policy, all major and mission-critical USADF information technology (IT) systems are now cloud-based and are delivered by cloud service providers approved through the FedRAMP.

USADF met or exceeded all CAP Goals for 2016 with the exception of Hardware and Software Asset Management.

## Independent Assessment

<b>Identify</b>	Level 1: Ad-Hoc
<b>Protect</b>	Level 1: Ad-Hoc
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 2: Defined
<b>Recover</b>	Level 2: Defined

The Office of Inspector General (OIG) contracted with an independent certified public accounting firm to conduct an audit to determine whether USADF implemented certain security controls for selected information systems in support of the FISMA. The firm tested USADF’s implementation of selected controls outlined in NIST’s Special Publication 800-53, Revision 4. The audit reviewed seven systems. Overall, USADF did not implement its information security program in support of FISMA. Specifically, USADF implemented only 41 of the 77 selected security controls. The audit made 26 recommendations to address the remaining controls to strengthen USADF’s information security program, including security assessments and authorizations, account management, asset management, and physical and environmental controls. The extent of the weaknesses in USADF’s information systems resulted in a significant deficiency to information system security again this year, as in FY 2015. Detailed audit findings and recommendations to address identified weaknesses are outlined in Audit Report No. A-ADF-17-002-C, which can be found on the OIG’s website.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	NA	0%
Software Asset Management	NA	0%
Vulnerability Management	✓ 100%	100%
Secure Configuration Management	✓ 100%	100%
Unprivileged User PIV Implementation	✓ 100%	100%
Privileged User PIV Implementation	✓ 100%	100%
Anti-Phishing Defenses	✓ 6	6
Malware Defenses	✓ 4	4
Other Defenses	✓ 3	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

American Battle Monuments Commission

## Chief Information Officer Assessment

The American Battle Monuments Commission's (ABMC) Board of Commissioners met to define a strategic plan, which will take the agency to its centennial in 2023. Among the focus areas, two were of highest importance: Operational Enhancement and Safety and Security and Welfare. Cybersecurity is at the crux of these focus areas, with ABMC's worldwide operations supported by a solid, secure, and efficient information technology (IT) infrastructure. ABMC is committed to developing and maturing its information systems security practices to ensure compliance with current cybersecurity requirements.

ABMC has met CAP Goals for Software Asset Management, Anti-Phishing, and Other Defenses.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 3: Consistently Implemented
- Respond** Level 2: Defined
- Recover** Level 2: Defined

FY 2016 is the first year ABMC has reported its FISMA metrics. Overall, ABMC has made great strides to ensure that its information security policies and procedures not only meet FISMA requirements, but also meet its overarching business needs. The agency has developed several plans of action and milestones (POA&Ms) to address FISMA requirements.

The scope of the evaluation included all aspects of ABMC's IT environment. Overall ABMC's information security program is effective, but can be improved upon. The primary reason for the "defined" state of ABMC's information security program is based on their lack of overall written policies, however during our testing and interviews with ABMC staff it was determined that for the five areas assessed a higher overall state would have been achieved based on actual implementation of ABMC's security program.

Our primary recommendation is to address the POA&Ms already identified and to ensure that the policies and procedure POA&Ms is successfully addressed in FY2017. We also recommended that ABMC ensure its IT environment is included in their annual ERM process.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	NA	80%
Software Asset Management	NA	✓ 100%
Vulnerability Management	NA	41%
Secure Configuration Management	NA	94%
Unprivileged User PIV Implementation	NA	0%
Privileged User PIV Implementation	NA	0%
Anti-Phishing Defenses	NA	✓ 6
Malware Defenses	NA	1
Other Defenses	NA	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 4

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	3
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Armed Forces Retirement Home

## Chief Information Officer Assessment

The Armed Forces Retirement Home (AFRH) met CAP Goals for Vulnerability Management, Anti-Phishing Defenses, and Malware and Other Defenses, while improving in Hardware Asset Management and Privileged User Personal Identity Verification (PIV) Implementation from FY 2015 to FY 2016.

## Inspector General Assessment

- Identify** Level 5: Optimized
- Protect** Level 3: Consistently Implemented
- Detect** Level 1: Ad-Hoc
- Respond** Level 2: Defined
- Recover** Level 3: Consistently Implemented

Reviewed for FISMA compliance were current testing activities for the AFRH system re-cert, documented in July through September 2016, and the assessment of Department of Interior (Interior) policies and processes for the administration and maintenance of the AFRH LAN. AFRH, in coordination with its vendor, Interior, has made significant progress in documenting and defining its security program. AFRH has some deficiencies in the areas of incident response and continuous monitoring. Although stakeholders and participants are identified in its Incident Response Plan, responsibilities for each role is not clearly defined, and a process for identifying lessons learned has not been developed. No process is defined for collecting quantitative measurements of performance in ISCM/IR. However, AFRH has made strides in developing a vendor management and assessment program to assist in validating compliance.

AFRH will continue working with Interior to ensure the documentation of and adherence to clear processes and procedures, specifically in the areas of continuous monitoring, incident response, and contingency planning. It will also work to ensure that documentation is complete and that AFRH remains in compliance with relevant policy.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	0%		
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%		
Privileged User PIV Implementation	0%		
Anti-Phishing Defenses	✓ 5	5	7
Malware Defenses	✓ 4	4	3
Other Defenses	✓ 4	4	3

### US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0





# Cybersecurity Performance Summary

Barry Goldwater Scholarship and Excellence in Education Foundation

## Chief Information Officer Assessment

The Barry Goldwater Scholarship and Excellence in Education Foundation (BGSEEF) actively works with the DHS to assure compliance and security. At this time, BGSEEF presents no independent security risk. Personnel and financial issues are contracted through the General Services Administration and the Department of Agriculture's Office of the Chief Financial Officer.

BGSEEF has entered into a contract for technical and cybersecurity support and maintenance, monitoring and reporting, including intrusion protection, firewall management and data loss prevention.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for BGSEEF was not performed for FY 2016 and this 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. BGSEEF will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	0%	0%	0%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	2%	0%	0%
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 5	5	5
Other Defenses	✓ 3	3	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Board of Governors of the Federal Reserve

## Chief Information Officer Assessment

Board of Governors of the Federal Reserve (FRB) has implemented and maintained an information security program that is consistent with FISMA requirements in all eight of the information security domains: risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring (ISCM), incident response, and contingency planning. The FRB follows a risk-based approach to continuously improve its information security program in all eight of the domains.

In 2016, the FRB continued to enhance its Information Security Continuous Monitoring and vulnerability management programs. In addition, the FRB met the CAP goal for Personal Identity Verification (PIV) enforcement of privileged users. In addition, the FRB met CAP Goals in 2016 for Vulnerability Management, Anti-Phishing, Malware Defense, and Other Defenses.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 3: Consistently Implemented

Overall, FRB continues to mature its information security program to ensure that it is consistent with FISMA requirements. The Inspector General also found that FRB's information security program includes policies and procedures that are generally consistent with the requirements for all eight information security domains. However, there are identified opportunities to strengthen controls in the areas of risk management, identity and access management, security and privacy training, and incident response, for which the audit report includes nine recommendations.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	90%	79%
Software Asset Management	0%	22%
Vulnerability Management	75%	100%
Secure Configuration Management	100%	0%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	5%	86%
Anti-Phishing Defenses	4	6
Malware Defenses	2	4
Other Defenses	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 9

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	0
Web	3
Other	4
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Broadcasting Board of Governors

## Chief Information Officer Assessment

The Broadcasting Board of Governors (BBG) is currently in the process of implementing the necessary frameworks to meet the July 2016 OMB A-123 requirements for an organization-wide Enterprise Risk Management (ERM) Program. The Office of the Chief Information Officer (OCIO) will address development and implementation of an organization-wide information technology (IT) security risk management strategy that aligns risk management decisions with business functions and objectives within the BBG's ERM Strategy. The OCIO has updated its IT Capital Planning and Investment Control program, policy, procedures, and staff training to account for agency-wide enterprise risk beyond the scope of investment risk alone. The most recent audit found that BBG did not fully develop and implement an organization-wide information security program to identify, protect, detect, respond to, and recover from information security weaknesses, using risk-based decision making, as evidenced by the control weaknesses identified in all eight key Inspector General (IG) FISMA metric domains.

BBG met CAP Goals for 2016 in Vulnerability Management, Anti-Phishing, Malware Defense, and Other Defenses.

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 1: Ad-Hoc
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 1: Ad-Hoc

The IG found that BBG did not fully develop and implement an organization-wide information security program to identify, protect, detect, respond to, and recover from information security weaknesses using risk-based decision making, which is evidenced by the control weaknesses identified in all eight key FISMA metric domains. The reason BBG did not have an effective information security program is in part because BBG did not devote the resources to fully develop and implement an organization-wide risk management strategy.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	5%	30%
Software Asset Management	5%	7%
Vulnerability Management	40%	95%
Secure Configuration Management	0%	0%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	6
Malware Defenses	3	3
Other Defenses	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 8

Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	7
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Chemical Safety Board

## Chief Information Officer Assessment

The Chemical Safety Board (CSB) was assessed pursuant to the FY 2016 FISMA. Five function areas identified by the NIST Framework for Improving Critical Infrastructure Cybersecurity were assessed, with the Identify and Recover function areas rated as Optimized. CSB's Protect and Detect function areas were rated as Consistently Implemented, and the Respond function was rated as Defined.

CSB met CAP Goals in FY 2016 for Hardware Asset, Software Asset, and Vulnerability Management, and Anti-Phishing, Malware, and Other Defenses.

## Inspector General Assessment

**Identify** Level 5: Optimized  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 2: Defined  
**Recover** Level 5: Optimized

CSB is considered effective in two of the five information security function areas. The EPA Office of the Inspector General assessed the five Cybersecurity Framework function areas and the corresponding metric domains as specified by the FY 2016 IG FISMA reporting metrics. Several areas within the CSB's information security program were identified as receiving a Not Met response, which affected the agency's rating and ability to achieve Level 4 of the maturity model. Based on our analysis, improvements are needed in the following areas:

- **Identity and Access Management:** CSB has not fully implemented the use of Personal Identity Verification cards for physical and logical access.
- **Security and Privacy Training:** CSB has not tracked the specialized training requirements for users with significant information security and privacy responsibilities, and has not measured the effectiveness of its security and privacy training.
- **Incident Response:** CSB has not identified or fully defined the incident response technologies it plans to use.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	0%	0%	0%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	36%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	0%
Anti-Phishing Defenses	4	5	5
Malware Defenses	✓ 2	4	4
Other Defenses	1	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Commission of Fine Arts

## Chief Information Officer Assessment

Commission of Fine Arts (CFA) is a small agency with a general support system (GSS) that received an Authorization to Operate (ATO) in 2013. Although vulnerabilities were discovered, the overall system security posture was deemed satisfactory. CFA's manageable number of privileged users and absence of significant personally identifiable information (PII) reduces risk of exploitation and limits the potential impact to the CFA GSS. CFA's security program has improved since receiving its ATO; since then, CFA has procured the services of an approved Managed Trusted Internet Protocol Service (MTIPS) provider. The MTIPS provider manages the sole circuit through which the CFA accesses internet services. The addition of a virtual private network allows CFA to safely access personnel and budgetary services from systems maintained by the Interior Business Center. Further, the EINSTEIN 3 Accelerated (E<sup>3</sup>A) Intrusion Prevention Security Services was integrated into the MTIPS service this past year. CFA recognizes that its internal controls require improvement.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for CFA was not performed for FY 2016 and this 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 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Hardware Asset Management	0%
Software Asset Management	0%
Vulnerability Management	0%
Secure Configuration Management	0%
Unprivileged User PIV Implementation	0%
Privileged User PIV Implementation	0%
Anti-Phishing Defenses	0
Malware Defenses	2
Other Defenses	0



## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Commission on Civil Rights

## Chief Information Officer Assessment

Since submitting last year's report, the USCCR continues toward full compliance with FISMA targets and with the agency's Privacy Management Program. The current number of reportable systems at the USCCR stands at 3. During FY 2016, the agency completed security assessments and approved change authorizations for each system. As a small agency without an Office of Inspector General, USCCR had contracted with a third-party service provider to assess the agency towards meeting the FISMA Metrics and Cybersecurity CAP goals. Subsequently, the third-party contractor identified weaknesses and program issues related to the five (5) areas of the FISMA CIO Metrics: Identify, Protect, Detect, Response and Recover. USCCR senior leadership is overseeing initiatives to address these findings.

Since submitting last year's FISMA and privacy management reports, the USCCR has had no major security incidents. None the minor incidents resulted in any compromise of personally identifiable information (PII), sensitive agency information, or information systems.

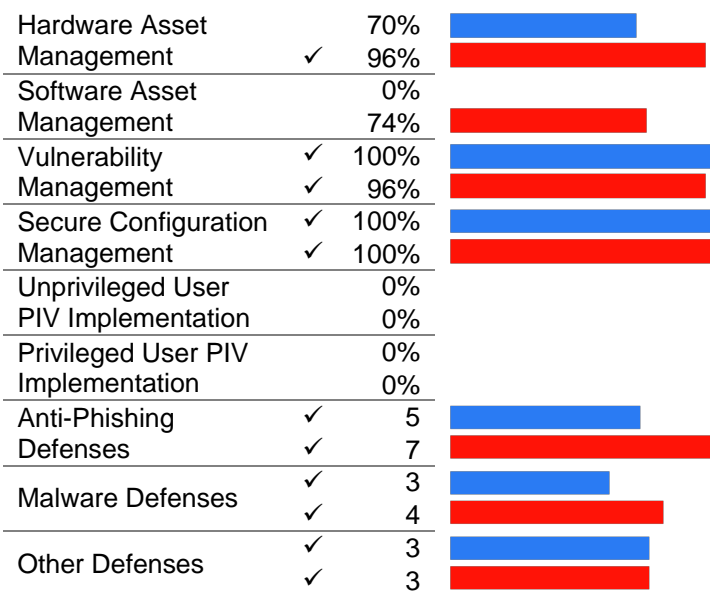
## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for USCCR was not performed for FY 2016 and this section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of Inspector General (OIG) appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. USCCR will explore contracting with an independent assessor in FY 2017.

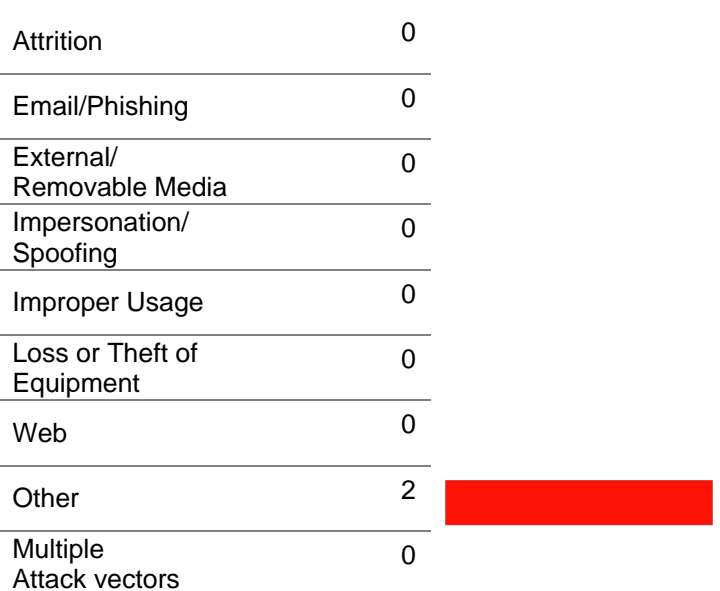
## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 2





# Cybersecurity Performance Summary

Committee for Purchase from People Who Are Blind or Severely Disabled

## Chief Information Officer Assessment

The Committee for Purchase from People Who Are Blind or Severely Disabled administers the AbilityOne program. AbilityOne is currently working to further build a more inclusive information security program following the guidelines outlined in NIST Special Publication 800-37, and other FISMA guidelines. As a micro-agency, it has been difficult to solicit and obtain adequate resources to support an organizational wide security program much like larger agencies, but AbilityOne is taking an aggressive approach to further train its current staff on FISMA compliance and obtaining new resources to further grow the program. AbilityOne has long-standing contracts with and Information Technology (IT) Security company to conduct our annual security assessments and utilizing industry experts to further build a fully compliant information security program. AbilityOne plans to make much progress in FY 2017 for its information security program and closing a large majority of its Plans of Action and Milestones.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 1: Ad-Hoc

There is partial evidence to conclude that the AbilityOne's Information Security Program sufficiently enforces Identification, Protection, Detection, Response and Recovery activities to improve system performance, decrease operating costs, increase security, and ensure public confidence in the confidentiality, integrity, and availability of information. The AbilityOne information technology enterprise appears to partially leave the data within the AbilityOne General Support System and Procurement List Information Management System enterprise application at increased potential for exploitation and risk of public data safety.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	100%
Software Asset Management	0%	100%
Vulnerability Management	0%	100%
Secure Configuration Management	84%	97%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	2	7
Malware Defenses	1	4
Other Defenses	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Commodity Futures Trading Commission

## Chief Information Officer Assessment

The Commodity Futures Trading Commission's (CFTC) information technology (IT) security program is managed and measurable. The program is effective and complies with the FISMA and OMB mandates, and it exemplifies numerous industry and government best practices. Given the evolving and complex nature of cyber threats and adversaries' constant targeting of government networks, it is imperative for CFTC to continuously improve and strengthen its security posture. To accomplish this, CFTC will institutionalize risk-based security policies and ensure enterprise compliance, expand and extend continuous monitoring capabilities, integrate Identity, Credential, and Access Management programs into the security program, assure a trusted and resilient information and communications infrastructure, and continue to improve anti-phishing and malware defense capabilities. The successful deployment of the aforementioned capabilities is an important foundation, which the CFTC will continue to develop as it enhances the protection of its information and infrastructure assets.

CFTC reported meeting all CAP Goals in FY 2016.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 5: Optimized  
**Respond** Level 4: Managed and Measureable  
**Recover** Level 5: Optimized

The Office of the Inspector General (OIG) witnessed a re-energized focus by CFTC to improve its cybersecurity posture. The OIG's audit results from information systems reviews revealed that management is addressing information security vulnerabilities. This increase in information security competency is demonstrated by the Office of Data and Technology's approach of reallocating staff, increasing the frequency of network scans, and patching vulnerabilities accordingly. During the year, CFTC's scan of sensitive databases showed that it was configured to minimize vulnerabilities and the risk of data loss.

To further improve its security posture, it is recommended that CFTC follow policies for physical access controls, extend its PIV program to external systems serviced by Federal partners, and mature an insider threat program.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	93%	100%	93%
Unprivileged User PIV Implementation	0%	0%	87%
Privileged User PIV Implementation	0%	100%	0%
Anti-Phishing Defenses	4	5	5
Malware Defenses	1	3	3
Other Defenses	3	3	3

### US-CERT Incidents by Attack vector

Total Number of Incidents: 2

Attack Vector	2015	2016
Attrition	0	0
Email/Phishing	0	0
External/Removable Media	0	0
Impersonation/Spoofing	0	0
Improper Usage	1	1
Loss or Theft of Equipment	0	0
Web	0	0
Other	1	1
Multiple Attack vectors	0	0



# cfpb Cybersecurity Performance Summary

Consumer Financial Protection Bureau

## Chief Information Officer Assessment

The Consumer Financial Protection Bureau (CFPB) continues to refine and mature its FISMA-based information security program to support the operational needs of the Bureau. The information security program is well established in policy with repeatable processes and effective controls that are integrated with the CFPB's risk management functions and aligned with our strategic objectives. The Inspector General (IG) concluded that the program is consistent with seven of the eight FISMA domains. CFPB is on-track to complete improvements in the final domain of contingency planning. Further, the IG closed six of the seven recommendations that were open at the start of this year's FISMA review cycle and CFPB continues to make progress toward closure on the seventh. CFPB is actively involved in the DHS's Continuous Diagnostics and Mitigation (CDM) program and awaiting deployment of the capabilities that the program is anticipated to provide. The CDM program will complement the CFPB's efforts to continuously refine processes and operations to further evolve the CFPB's Information Security Continuous Monitoring (ISCM) program. CFPB anticipates a steady tempo of progress throughout FY 2017. CFPB is excited to launch a new cybersecurity training and awareness program in FY 2017 that will equip the CFPB workforce with the tools and knowledge needed to help protect the CFPB's systems and data from cyber threats.

## Inspector General Assessment

**Identify** Level 4: Managed and Measureable  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

Overall, the IG found that the CFPB continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the CFPB has implemented several tools to automate ISCM capabilities, matured its ISCM program from Level 1, Ad Hoc to Level 3, Consistently Implemented, and strengthened its role-based training program for users with significant security responsibilities. The IG also found that the CFPB's information security program is generally consistent with seven of the eight information security domains listed by DHS: risk management, contractor systems, configuration management, identity and access management, security and privacy training, ISCM, and incident response. For the remaining domain, contingency planning, the CFPB has not completed an agency-wide business impact analysis to guide its contingency planning activities, nor has it fully updated its continuity of operations plan to reflect the transition of its information technology infrastructure from the Department of the Treasury.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	34%
Software Asset Management	0%	0%
Vulnerability Management	95%	90%
Secure Configuration Management	100%	21%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	3
Malware Defenses	3	3
Other Defenses	1	1

### US-CERT Incidents by Attack vector

Total Number of Incidents: 152

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	5
Loss or Theft of Equipment	108
Web	15
Other	22
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Consumer Product Safety Commission

## Chief Information Officer Assessment

The Consumer Product Safety Commission (CPSC) has shown progress and is on target to strengthen its cybersecurity posture. For example, CPSC added cybersecurity resources to the agency staff and hired a Chief Information Officer with a strong cybersecurity background in FY 2016 as reported in the Office of Inspector General report.

CPSC met the Secure Configuration Management and Anti-Phishing Defense CAP Goals in FY 2016. CPSC did not meet the Unprivileged User Personal Identity Verification (PIV) CAP Goal in FY 2016, despite having met the goal in FY 2015.

PIV enforcement was temporarily suspended in FY 2016 due to conflicts with the agency's patch management processes. However, the use of PIV or NIST Level of Assurance 4 credentials for unprivileged user access remains the standard access method for agency information systems. PIV enforcement is planned for restoration in FY 2017.

## Inspector General Assessment

**Identify** Level 1: Ad-Hoc  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 2: Defined  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 1: Ad-Hoc

CPSC improved its policies and procedures, implemented new cybersecurity solutions, and is actively working toward standardizing its risk documentation. These improvements resulted in the achievement of Level 2, Defined, of the Information Security Continuous Monitoring maturity model. CPSC remains at Level 1 of the Incident Response maturity model. CPSC has not: developed and maintained a comprehensive software and hardware inventory; documented and implemented baseline configurations for all agency hardware and software; applied patches in a timely manner; enforced multi-factor authentication; properly applied the Principle of Least Access; developed and maintained a business impact assessment and contingency and continuity plans; provided role-based security and privacy training to all applicable agency resources; implemented an organization-wide risk management program; or established and properly updated existing Interconnection Security Agreements for all CPSC third-party systems. Information Technology contracts and agreements for goods and services lack required Federal Acquisition Regulation clauses and/or other provisions.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	68%	25%
Software Asset Management	0%	60%
Vulnerability Management	54%	75%
Secure Configuration Management	✓ 100%	✓ 100%
Unprivileged User PIV Implementation	✓ 100%	8%
Privileged User PIV Implementation	0%	3%
Anti-Phishing Defenses	4	✓ 5
Malware Defenses	0	1
Other Defenses	✓ 2	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 10

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	2
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	3
Other	5
Multiple Attack vectors	0

# Cybersecurity Performance Summary

Corporation for National and Community Service

## Chief Information Officer Assessment

The Corporation for National and Community Service's (CNCS) cybersecurity program continues to integrate security processes, procedures, and protections into a wide range of data systems that support the agency. Working closely with system owners and support contractors, the cybersecurity program has raised awareness and has vastly improved its information security program over the last year. CNCS is steadily moving towards a continuous monitoring methodology for all systems and cloud services. In addition, CNCS is preparing to accept the Continuous Diagnostics and Monitoring (CDM) program sponsored by the DHS. During a self-assessment for CDM CNCS discovered that the current method of identifying hardware assets was initiated manually versus automatically. That discovery caused the shift from 95% to 0% for hardware asset management reporting. In the interim CNCS has plans to conduct full hardware inventory twice during 2017 and implement network discovery scans at least quarterly. CNCS has been able to correct multiple deficiencies that were identified by its Inspector General evaluation, and it continues to plan information technology (IT) projects that incorporate cybersecurity to safeguard information critical to the agency.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 2: Defined
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 2: Defined
<b>Recover</b>	Level 1: Ad-Hoc

CNCS has taken a number of steps to address information security and privacy weaknesses from the FY 2015 FISMA evaluation, fully resolving eight of 17 findings from the FY 2015 evaluation and closing 67 of 90 open prior-year recommendations. These steps include updating policies and procedures for key security program areas, including information security continuous monitoring, risk management, and Plan of Action and Milestones management. CNCS has also developed service level agreements with its primary IT contractor, who manages CNCS's desktops, servers, and network infrastructure.

While the Corporation has matured its Security and Privacy Program, Evaluators uncovered two new weaknesses: 1) secure configuration management policies, procedures, and practices need improvement and 2) insufficient monitoring and remediation of server backup failures. Of the 57 security metrics in the six domains without a maturity model, our testing identified 25 instances of noncompliance with applicable laws, regulations, and authoritative guidance governing information security.

## CAP Goal Metrics

✓ CAP Goal Met      ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 95%	95%	0%
Software Asset Management	60%	60%	100%
Vulnerability Management	10%	10%	67%
Secure Configuration Management	✓ 100%	100%	68%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	0%
Anti-Phishing Defenses	3	3	6
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 2	2	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 25

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	4
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	14
Web	1
Other	5
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Council of the Inspectors General on Integrity and Efficiency

## Chief Information Officer Assessment

The Council of the Inspectors General on Integrity and Efficiency (CIGIE) is setting up its information technology (IT) security program, and as such does not yet have robust capabilities. These are being designed into the architecture with the assistance of the DHS, specifically the Continuous Diagnostics and Mitigation (CDM) program.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for CIGIE was not performed for FY 2016 and this 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. CIGIE will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Hardware Asset Management	NA	0%
Software Asset Management	NA	0%
Vulnerability Management	NA	0%
Secure Configuration Management	NA	0%
Unprivileged User PIV Implementation	NA	0%
Privileged User PIV Implementation	NA	0%
Anti-Phishing Defenses	NA	5
Malware Defenses	NA	0
Other Defenses	NA	1



## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Court Services and Offender Supervision Agency

## Chief Information Officer Assessment

The Court Services and Offender Supervision Agency (CSOSA) has made significant strides in advancing the CSOSA Information Security Continuous Monitoring (ISCM) Strategy through the implementation of CSOSA's ISCM program and capabilities. CSOSA has identified and acquired new tools and additional staff, and it has started to implement capabilities to automate the collection, analysis, and reporting of security-related information that will allow for the seamless transition to ongoing authorization. CSOSA continues to make considerable progress implementing capabilities to detect hardware and software devices, and plans to expand the use of Personal Identity Verification (PIV) cards across the enterprise. As a result, CSOSA did meet three CAP Goal metrics despite the limited reporting capabilities available. Additionally, in FY 2017, CSOSA will be implementing a centralized incident response capability, which will include the improvement of CSOSA's agency-wide security operations center.

## Independent Assessment

<b>Identify</b>	Level 1: Ad-Hoc
<b>Protect</b>	Level 1: Ad-Hoc
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 1: Ad-Hoc

Overall, the external independent auditor found CSOSA has made progress in addressing previously identified information security improvements; however, the independent external auditor identified areas of improvements highlighted from previous years' audits that are still being addressed. Further, the external independent auditor found additional areas of improvement in FY 2016 as reported to the Agency Director. The external independent auditor determined that the Agency achieved the maximum points for the Level 1, Ad-hoc, maturity level in almost all Cybersecurity Framework Security Functional areas when measuring the effectiveness of the Agency information security program and practices; however in the Detect functional area, the Agency achieved a Level 2, Defined, maturity level, which is consistent with the importance the Agency has placed in FY 2016 on maturing the Information Security Continuous Monitoring program.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	0%
Vulnerability Management	66%	100%
Secure Configuration Management	65%	0%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	2	6
Malware Defenses	1	1
Other Defenses	1	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Defense Nuclear Facilities Safety Board

## Chief Information Officer Assessment

Defense Nuclear Facilities Safety Board's (DNFSB) information technology (IT) environment continued to improve its information security posture during FY 2016. Positive progress was made in development of information security policies and plans. The execution of the information security policies have been hindered by personnel shortfalls, including the position of the Chief Information Security Officer and qualified cybersecurity and information assurance personnel. The agency addressed the shortfall in cybersecurity and information assurance by hiring a contractor full-time equivalent Senior Information Assurance Manager in September 2016. The agency is working with the DHS Continuous Diagnostics and Mitigation (CDM) Tools and Sensors program office to strengthen the DNFSB network. DNFSB has also procured several automated toolsets to assist in securing data-at-rest and increasing the monitoring capability of the agency's network enterprise.

In FY 2017, DNFSB will focus on the execution and sustainment of the continuous monitoring and detection processes and the deployment and business normalization of automated tools. The agency will strengthen its cybersecurity and information assurance workforce to the maximum extent possible.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 1: Ad-Hoc

DNFSB information security program is generally effective. Policies and procedures have been developed for the eight topic areas in the Office of Inspector General metrics. The DNFSB general support system underwent a full security assessment in FY 2016, with the authorization to operate (ATO) issued in November 2015. In FY 2016, DNFSB completed implementation of all nine recommendations from the FY 2014 independent evaluation: five in November 2015, two in July 2016, and the final two at the end of fieldwork for this year's assessment. As the implementation of the recommendations has been less than six months, there is not sufficient information to measure their effectiveness. DNFSB is in CDM Group F. Task order 2F is scheduled for deployment in FY 2017 and includes deployment of an agency's Information Security Continuous Monitoring dashboard.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	31%
Vulnerability Management	0%	100%
Secure Configuration Management	77%	99%
Unprivileged User PIV Implementation	0%	100%
Privileged User PIV Implementation	0%	100%
Anti-Phishing Defenses	5	4
Malware Defenses	1	5
Other Defenses	3	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Denali Commission

## Chief Information Officer Assessment

Denali Commission (Denali) uses the United States Treasury Shared Services systems. The Agency does not collect personally identifiable information (PII) and systems collecting private data are not housed at the Agency.

## Inspector General Assessment

**Identify** Level 1: Ad-Hoc  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 1: Ad-Hoc

Denali is a relatively small agency that relies upon the shared services provider, the Department of the Treasury's Bureau of Fiscal Services, to provide much of their information technology (IT) security. 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 the identify, protect, detect, respond, and recover components of the NIST Information Security 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.

## CAP Goal Metrics

✓ CAP Goal Met ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	0%
Vulnerability Management	0%	0%
Secure Configuration Management	✓ 100%	100%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	0	✓ 5
Malware Defenses	0	✓ 3
Other Defenses	0	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Department of Agriculture

## Chief Information Officer Assessment

Department of Agriculture (USDA) has vibrant and effective information technology (IT) cybersecurity and Privacy Act programs. The Department is committed to supporting IT cybersecurity as a living entity with our everyday operations; from alignment of the Cybersecurity Strategic Plan to the USDA's overall Strategic Business Plan, and the collaborative work enterprise-wide to implement these strategic plans. USDA has established operations to identify, protect, detect, respond and recover to IT security requirements and issues enterprise-wide. USDA has implemented a strong IT Risk Management framework to identify and manage cybersecurity risk to systems, assets, data, and capabilities. The program begins at the investment level and follows through to the day-to-day implementation of cybersecurity controls and continuous monitoring across the Department. USDA integrates appropriate safeguards to protect and limit the impact of cybersecurity events using controls outlined by NIST Special Publication 800-53, OMB and other Federal regulations, including, but not limited to: Access Control; IT Security Awareness Training for all employees, contractors, volunteers, and partners; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology. The annual training is reinforced through quarterly phishing exercises through the year.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 1: Ad-Hoc
- Respond** Level 2: Defined
- Recover** Level 2: Defined

The Office of the Chief Information Officer (OCIO) continues to take positive steps towards improving USDA's security posture, releasing two critical policies this year: Secure Communication Systems and Contingency Planning and Disaster Recovery Planning. Once implemented, these policies should improve IT security within USDA. OCIO also began implementing the Continuous Diagnostics and Mitigation (CDM) program tools. Although USDA is working to improve its IT security posture, many longstanding weaknesses remain. OCIO has not implemented corrective actions committed to in response to prior Office of Inspector General (OIG) recommendations. In FYs 2009 - 2015, OIG made 61 recommendations for improving the overall security of USDA's systems; 39 have been closed and 22 remain open for completion. Testing identified that security weaknesses still exist in 3 of 39 closed recommendations. The OIG continues to report a material weakness in USDA's IT security that should be included in USDA's Federal Managers Financial Integrity Act report and concludes that USDA lacks an effective information security program and practices.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 95%	95%	95%
Software Asset Management	✓ 100%	100%	99%
Vulnerability Management	85%	95%	95%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 86%	86%	89%
Privileged User PIV Implementation	89%	89%	96%
Anti-Phishing Defenses	✓ 6	6	5
Malware Defenses	0	0	4
Other Defenses	✓ 2	2	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,867

Attack Vector	Number of Incidents
Attrition	4
Email/Phishing	27
External/Removable Media	1
Impersonation/Spoofing	3
Improper Usage	293
Loss or Theft of Equipment	155
Web	381
Other	962
Multiple Attack vectors	41





# Cybersecurity Performance Summary

Department of Commerce

## Chief Information Officer Assessment

The Department of Commerce (Commerce) worked aggressively in FY 2016 to enhance its information technology (IT) security posture and improve its performance on the CAP Goals and other FISMA areas. In FY 2016, Commerce met seven CAP Goal targets, up from six in FY 2015. Overall, Commerce improved across 14 of the 24 CAP metrics. The largest increases were noted in Anti-Phishing and Malware Defense due to more pervasive deployment of tools for intrusion prevention, e-mail authentication protocols, detonation chambers, and leveraging an enterprise anti-phishing license. In FY 2016, every bureau conducted anti-phishing exercises. Commerce continues to mature its automated Hardware Asset Management capabilities. It will also be employing whitelisting for software application management. Focused efforts on Commerce's Identity, Credential, and Access Management (ICAM) initiatives resulted in progress department-wide. Commerce is participating in Personal Identity Verification Interoperability (PIV-I) pilots to increase performance. An enterprise view of the real-time security posture of Commerce's systems is being enabled through the Enterprise Cybersecurity Monitoring and Operations program and Enterprise Security Operations Center. Additional monitoring tools will be integrated in FY 2017 as a result of Commerce's participation in the Continuous Diagnostics and Mitigation (CDM) Program.

## Inspector General Assessment

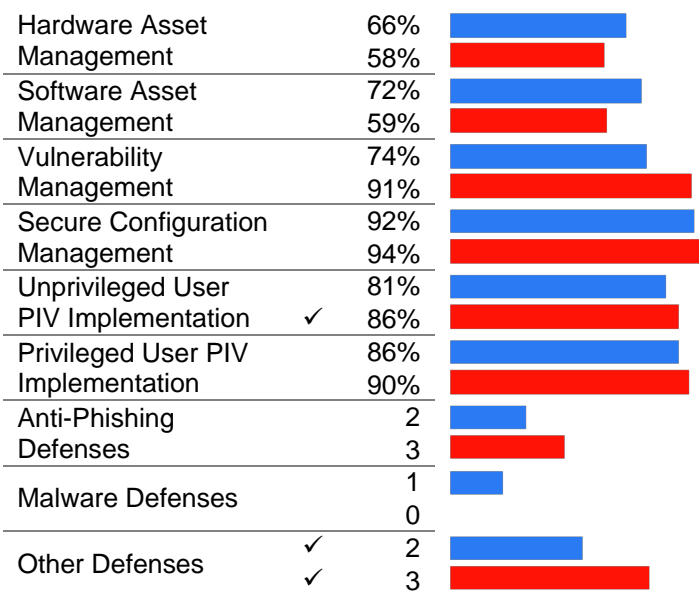
**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 2: Defined  
**Recover** Level 3: Consistently Implemented

The Office of Inspector General (OIG) completed an audit of Commerce's FISMA compliance by assessing the effectiveness of Commerce's information security program and practices. OIG also reviewed a representative subset of 18 IT systems from five of Commerce's Operating Units to assess compliance.

OIG's assessments of risk management, contractor systems, ICAM, Secure Configuration Management, Information Security Continuous Monitoring (ISCM), Incident Response, and contingency planning found that Commerce has largely defined the needed policy and procedures. OIG did find that overall contingency planning and security awareness training are consistently implemented. However, ICAM and ISCM security controls are not fully implemented. Commerce continues to struggle to effectively select, implement, and assess security controls to protect its information systems.

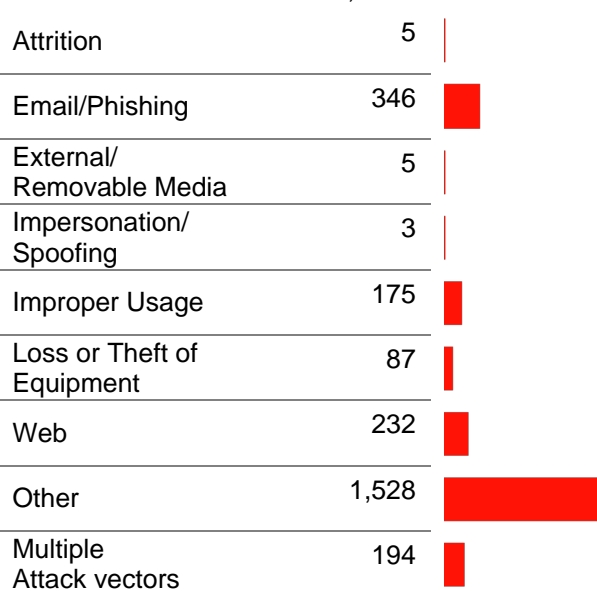
### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016



### US-CERT Incidents by Attack vector

Total Number of Incidents: 2,575





# Cybersecurity Performance Summary

Department of Defense

## Chief Information Officer Assessment

While the Department of Defense (DoD) faces many challenges due to its mission and size, the challenges in cybersecurity and information technology remain one of its highest priorities. DoD's Chief Information Officer (CIO) recently identified efforts to ensure that implementing the information security program is fully embraced by all Components, beginning at the individual level.

The CIO further stated that the DoD is working to transform its cybersecurity culture by improving human performance and accountability through a prioritized list of key cyber efforts known as the Cybersecurity Discipline Implementation Plan. The plan provides a roadmap to aggressively eliminate preventable cyber vulnerabilities that can put DoD missions at risk.

\*\* OMB is submitting DoD's FY 2016 metrics as part of a classified annex in accordance with 44 USC § 3554 (c)(1).

## Independent Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 2: Defined  
**Recover** Level 2: Defined

Overall, our assessment of the DoD's effectiveness of its information security program was scored at the maturity level of Defined for four of the five information security functions: Identify, Protect, Respond, and Recover. DoD policies, procedures, and strategies are not consistently implemented across the Department. Based on the maturity levels that our assessment for each information security function equated to, DoD's information security program did not receive an effective rating.

In FY 2016 Inspector General Summary of Management and Performance Challenges, we identified that the Commander, U.S. Cyber command, stated that while DoD has made progress in developing strategies and goals to combat cyber threats, the DoD continues to face significant challenges in increasing its overall cyber capabilities.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	83%	NA**
Software Asset Management	82%	NA
Vulnerability Management	20%	NA
Secure Configuration Management	0%	NA
Unprivileged User PIV Implementation	✓ 86%	NA
Privileged User PIV Implementation	51%	NA
Anti-Phishing Defenses	3	NA
Malware Defenses	1	NA
Other Defenses	✓ 2	NA

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,888

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	377
External/Removable Media	13
Impersonation/Spoofing	3
Improper Usage	249
Loss or Theft of Equipment	187
Web	159
Other	771
Multiple Attack vectors	129



# Cybersecurity Performance Summary

Department of Education

## Chief Information Officer Assessment

The Department of Education (ED) continues to make progress in strengthening its information security program and maintaining compliance with the requirements of FISMA. ED has prioritized its efforts on completing the actions specified in OMB Memorandum M-16-04, the Cybersecurity Strategy and Implementation Plan, and is making progress in achieving the President's Cybersecurity CAP Goal targets. ED has taken a number of steps to strengthen the cybersecurity posture of its networks and systems, to include implementing the DHS's recommendations for enhancing the security posture of the Federal Student Aid (FSA) environment, working to resolve all FISMA and financial audit findings, executing against ED's plans to implement the Federal Information Technology Acquisition Reform Act (FITARA) in a timely manner, and continuing key activities to retire outdated legacy information technology (IT) systems. ED established a high value asset list, including priority efforts in progress, to protect those assets using several cybersecurity tools, technologies, and processes. ED successfully implemented two-factor authentication for all external users of its customer-facing grants management system.

## Inspector General Assessment

**Identify** Level 5: Optimized  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 5: Optimized

The Office of Inspector General (OIG) reviewed ED's and FSA's IT security programs. OIG found that the overall IT security programs of ED and of FSA are deemed generally not effective. Although ED and FSA were generally effective in the Identify and Recover functions, they were not generally effective in the Protect, Detect, and Respond functions. Within the eight metric domains, findings were identified in five areas: (1) Configuration Management (Protect), (2) Identity Control and Access Management (Protect), (3) Security and Privacy Training (Protect), (4) Information Security Continuous Monitoring (Detect), and (5) Incident Response (Respond). The OIG report contains 11 findings, 5 of which are repeat findings from previous FISMA reports, and outlines 15 recommendations, 6 of which are repeat recommendations. Although the Department and FSA may have taken action on specific findings from previous FISMA reports, systemic issues in some metric domains persist year to year. Further details can be found in the final report (ED-OIG/A11Q0001) on ED's website.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Metric	2015	2016
Hardware Asset Management	77%	88%
Software Asset Management	17%	87%
Vulnerability Management	85%	100%
Secure Configuration Management	94%	100%
Unprivileged User PIV Implementation	78%	97%
Privileged User PIV Implementation	12%	100%
Anti-Phishing Defenses	5	7
Malware Defenses	1	1
Other Defenses	0	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 291

Attack Vector	Number of Incidents
Attrition	1
Email/Phishing	9
External/Removable Media	2
Impersonation/Spoofing	0
Improper Usage	89
Loss or Theft of Equipment	50
Web	11
Other	116
Multiple Attack vectors	13



# Cybersecurity Performance Summary

Department of Energy

## Chief Information Officer Assessment

The Department of Energy (Energy) implements its Cyber Strategy in several ways, including an enterprise-distributed, shared risk management framework and coordinated leadership, management, and governance of cyber activities and cyber-related issues. Energy monitors progress toward FISMA metrics and CAP Goal targets, paying special attention to the effectiveness of information security programs and practices. Energy's CAP Goal results are stable or have increased, and improvements are evident for Vulnerability Management and Personal Identity Verification (PIV) card usage for Privileged and Unprivileged Users. FY 2017 goals are set to show continued progress and commitment, particularly in Anti-Phishing and Malware Defense. Energy currently has not met Multifactor Authentication/ NIST Level of Assurance 4 compliance for Privileged Users and for Unprivileged Users however, significant increases projected by early FY 2017. Energy is deploying Continuous Diagnostics Mitigation (CDM) Phase 1 Endpoint Integrity tools in the Energy Information Technology Services and Office of Science environments, and it is fully engaged in Phase 2. Energy began implementing an integrated Joint Cybersecurity Coordination Center to unify cyber expertise and provide a collaborative, intelligence-driven, distributed approach to cyber operations and response. The Center achieved Initial Operating Capability in August 2016.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 1: Ad-Hoc

The Office of Inspector General (OIG) conducted the annual evaluation of Energy's unclassified information security program and reviewed the Department's information systems at six sites to assess the effectiveness of unclassified information security policies, procedures, and practices. Overall, the OIG determined that Energy was 'Not Effective' in the five information security functions: Identify, Protect, Detect, Respond, and Recover. Specifically, the OIG found that the Department was at Level 2: Defined for the Identify and Protect functions. In addition, the OIG determined that the Department was at Level 1: Ad-Hoc for the Detect, Respond, and Recover functions. Furthermore, the OIG determined that stakeholders may not have adequate people, processes, and technology resources to effectively implement both Information Security Continuous Monitoring and Incident Response activities throughout the Department.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015 (%)	2016 (%)
Hardware Asset Management	87%	60%
Software Asset Management	39%	44%
Vulnerability Management	31%	64%
Secure Configuration Management	92%	77%
Unprivileged User PIV Implementation	12%	53%
Privileged User PIV Implementation	10%	82%
Anti-Phishing Defenses	3	2
Malware Defenses	0	0
Other Defenses	0	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 620

Attack Vector	Number of Incidents
Attrition	8
Email/Phishing	99
External/Removable Media	4
Impersonation/Spoofing	7
Improper Usage	80
Loss or Theft of Equipment	197
Web	151
Other	73
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Department of Health and Human Services

## Chief Information Officer Assessment

Department of Health and Human Services (HHS) has made considerable progress in prioritizing and implementing security initiatives not only to align with the CAP Goal targets, but also with the Cybersecurity Act of 2015 and the Cybersecurity National Action Plan. In particular, HHS has improved its Cyber Hygiene capabilities to patch critical vulnerabilities, implemented a program to review the security protections on our High Value Assets, and significantly increased the use of Personal Identity Verification (PIV) credentials. HHS is moving forward with the Continuous Diagnostics and Mitigation (CDM) program and has procured additional tools that will enhance the program. HHS has been working with the DHS to develop the capability “to share cyber threat indicators and defensive measures in real time...”. HHS was the first Federal agency to authorize a Cloud Service Provider (CSP) and has continued to grant authorizations to operate (ATO) to eleven CSPs as a means of fostering cloud adoption across the Federal Government. During 2016, HHS implemented a robust anti-phishing program and developed the CyberCare program to disseminate security information to our staff. A new HHS information technology (IT) Strategic Plan was developed, which not only fosters the importance of the Federal Information Technology Acquisition Reform Act (FITARA), but also articulated a vision in the delivery of IT to enable the mission.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 2: Defined  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

HHS has made overall improvements and continues to implement changes to strengthen its information security program. HHS is aware of opportunities to strengthen information security in: continuous monitoring, configuration management, identity and access management, risk management, incident response, security training, and contingency planning. HHS formalized its Information Security Continuous Monitoring (ISCM) program through ISCM policies, procedures, and strategies. HHS continues to work towards implementing a department-wide CDM program to include continuously monitoring networks and systems, updating and finalizing policies and procedures, documenting Operating Division’s (OPDIV) progress to address and implement strategies and reporting through DHS dashboards. HHS also needs to ensure that all OPDIVs consistently review and remediate or address the risk presented by vulnerabilities, consistently implement account management procedures, and accurately track systems to ensure they are operating with a current and valid ATO. This will strengthen the program and further enhance the HHS mission

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	92%	77%
Software Asset Management	32%	34%
Vulnerability Management	82%	94%
Secure Configuration Management	76%	98%
Unprivileged User PIV Implementation	✓ 89%	✓ 89%
Privileged User PIV Implementation	98%	99%
Anti-Phishing Defenses	✓ 5	✓ 5
Malware Defenses	0	2
Other Defenses	✓ 2	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 8,121

Attack Vector	Number of Incidents
Attrition	6
Email/Phishing	693
External/Removable Media	9
Impersonation/Spoofing	7
Improper Usage	1,445
Loss or Theft of Equipment	884
Web	1,458
Other	3,466
Multiple Attack vectors	153



# Cybersecurity Performance Summary

Department of Homeland Security

## Chief Information Officer Assessment

The Department of Homeland Security (DHS) has made considerable progress in FY 2016. DHS has met five out of the nine CAP Goals, three more than the two met in FY 2015. The goals are Vulnerability Management, Unprivileged Mandatory PIV, Anti-Phishing Defense, Malware Defense, and Other Defenses. Additionally, DHS increased its score for two of the metrics: Hardware Asset Management and Software Asset Management. These results reflect DHS's focused efforts on improving over the FY, including quarterly cybersecurity update meetings with each Component's Executives, led by the Deputy Under Secretary for Management, which brought attention to particular areas of concern. The DHS Chief Information Officer has also improved tracking of capabilities across the department. DHS' quarterly cybersecurity assessments show consistent increases in DHS scores, which reflects the maturation of processes and practices within the cybersecurity community at DHS. Leveraging the Defense-in-Depth model, DHS developed a Cybersecurity Maturity Model which provides a standard method for assessing maturity throughout DHS and better guide funding to close gaps and accelerate maturity where needed.

## Inspector General Assessment

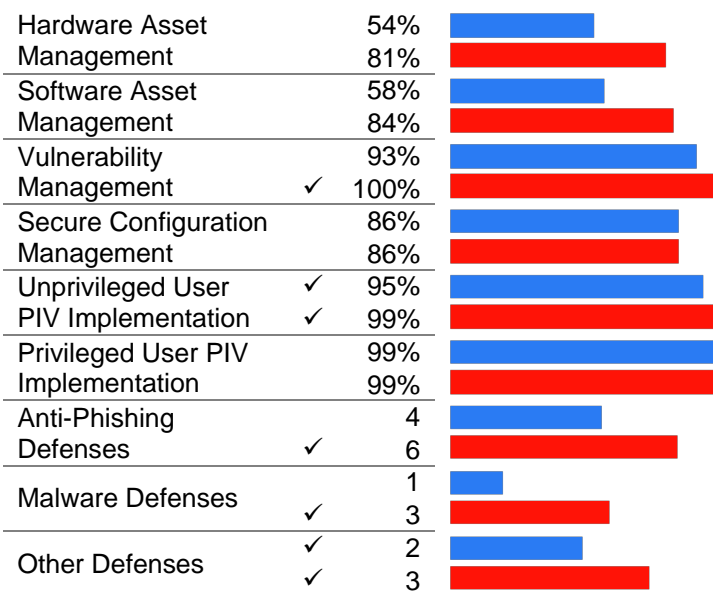
**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

DHS has taken actions to strengthen its information security program. In January 2016, the Under Secretary for Management issued a memorandum requiring components to enhance DHS's Cyber Defense by providing security training and exercises for employees and contractors, and by implementing endpoint protection solutions and two-factor authentication on DHS's classified networks. As of May 2016, all components were reporting information security metrics to the Department.

Despite the progress made, components were not consistently following DHS's policies and procedures to maintain current or complete information on remediating security weaknesses in a timely manner. Components operated 79 unclassified systems with expired Authorization to Operate (ATO). Components have not consolidated all internet traffic behind the Department's trusted internet connections and have continued to use unsupported operating systems. At this time, the Department cannot ensure that its systems are adequately secured to protect the sensitive information stored and processed in them.

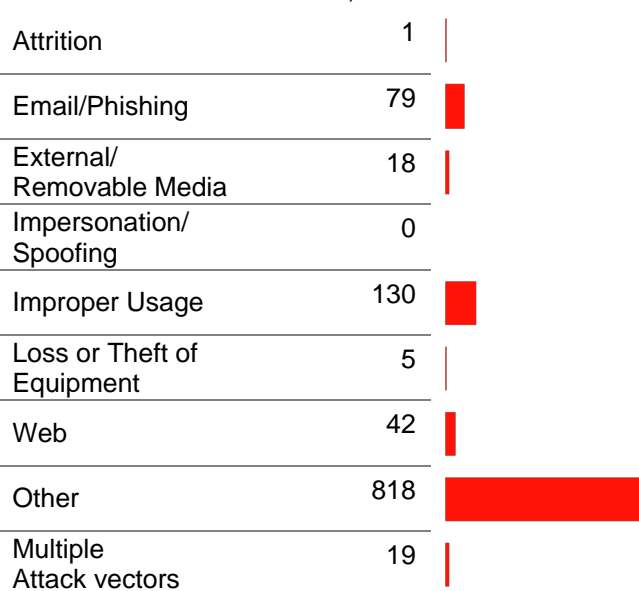
## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,112





# Cybersecurity Performance Summary

Department of Housing and Urban Development

## Chief Information Officer Assessment

The Charter for the Department of Housing and Urban Development (HUD) Security Council is being reviewed to establish physical and cybersecurity governance for the Department. HUD has established an Insider Threat Working Group, which is drafting an Insider Threat Policy. HUD is leveraging products offered by the DHS to assist with its establishment of the Insider Threat Program. HUD was able to take advantage of one of the free threat intelligence offerings from DHS and is acquiring tools to enable automation of syslog reviews and analysis for both inside and outside threats. HUD is in the process of procuring Cyber Independent Verification and Validation and penetration services to evaluate the effectiveness of the cyber program.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 3: Consistently Implemented
- Detect** Level 2: Defined
- Respond** Level 2: Defined
- Recover** Level 2: Defined

The Office of the Inspector General finds that the HUD cybersecurity practices and programs lacked consistent implementation. Key deficiencies include inadequate governance, risk management, and contractor system oversight functions. To mature its program, HUD must consistently define and implement standard processes and tools throughout the HUD enterprise and stand up a proper governance and compliance program. Some aspects of these functions, such as enterprise risk management and contracting procedures, are beyond the control of the Office of the Chief Information Officer (OCIO). Therefore, it is critical that HUD provide oversight and take action at and above the OCIO level. Overall, HUD has taken many notable steps to define and strengthen its cybersecurity program by developing more robust and enterprise-wide policies and procedures, establishing information security roadmaps, and planning implementation of additional tool and process capabilities. During the past two fiscal years, HUD made improvements in multiple domains such as Incident Response, Information Security Continuous Monitoring, and Configuration Management.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	62%	62%	99%
Software Asset Management	0%	90%	90%
Vulnerability Management	76%	100%	100%
Secure Configuration Management	100%	99%	99%
Unprivileged User PIV Implementation	95%	95%	95%
Privileged User PIV Implementation	100%	100%	100%
Anti-Phishing Defenses	6	6	6
Malware Defenses	4	4	3
Other Defenses	4	4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 86

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	20
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	2
Loss or Theft of Equipment	2
Web	1
Other	56
Multiple Attack vectors	5



# Cybersecurity Performance Summary

Department of Justice

## Chief Information Officer Assessment

The Department of Justice (Department) made significant advances in FY 2016 in the Department's cybersecurity capabilities to address the rapidly changing cyber threat landscape. The Department has implemented and continues to manage several solutions which have resulted in considerable cost avoidance by thwarting adversaries' attempts to breach the Department's network, gain access to sensitive information, and critically harm national security. These tools include memory analysis capabilities on critical endpoints which allows deep analysis to detect attacks; a data loss prevention capability for email and web traffic, which prevents the loss of sensitive data via the Department's email system and detects and blocks malicious web traffic; and automated malware detection at the internet perimeter to block malicious files, links, and spear-phishing attempts. As a result of these efforts and accomplishments, the cyber risk to the Department has decreased, avoiding damage of public image, loss of data, and the diversion of critical resources toward system remediation efforts instead of mission execution.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 4: Managed and Measureable

During FY 2016, the Justice Office of the Inspector General (OIG) reviewed the information security programs of six Department components and a sample of 12 systems within these components. As a result of the review, the OIG determined that the maturity level for the Department's information security program is Level 3, Consistently Implemented, across the first four Security Functions: Identify, Protect, Detect, and Respond; and Level 4, Managed and Measurable, for the fifth Security Function: Recover. During the review, the most findings were noted across all six components in the following domains: Configuration Management, Identity and Access Management, Security and Privacy Training (Protect), Information Security Continuous Monitoring (Detect), and Incident Response (Respond). In addition, findings were noted within four of the components for Risk Management (Identify) and within three of the components for Contingency Planning (Recover).

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 97%	97%	97%
Software Asset Management	✓ 97%	97%	98%
Vulnerability Management	✓ 97%	97%	98%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	64%	64%	57%
Privileged User PIV Implementation	65%	65%	64%
Anti-Phishing Defenses	4	4	6
Malware Defenses	✓ 3	3	3
Other Defenses	1	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 3,301

Attack Vector	Number of Incidents
Attrition	1
Email/Phishing	119
External/Removable Media	3
Impersonation/Spoofing	0
Improper Usage	685
Loss or Theft of Equipment	2,022
Web	144
Other	313
Multiple Attack vectors	14





# Cybersecurity Performance Summary

Department of Labor

## Chief Information Officer Assessment

Actions taken by the Department of Labor (Labor) Office of the Chief Information Officer (OCIO) cybersecurity program over recent years have been purposefully prioritized in accordance with the OCIO's overarching cybersecurity strategy. The strategy calls for the bolstering of foundational underpinnings of the enterprise program.

Examples of this include Labor's successful implementations of department-wide Personal Identity Verification (PIV) enforcement, enterprise patch management, EINSTEIN 3 Accelerated (E<sup>3</sup>A), Continuous Diagnostics and Mitigation (CDM) Phase 1 tools, a pilot of the CDM security dashboard, and acquisition of an identity access management solution suite that includes Privileged Identity Management.

Labor plans to leverage prior year successes in FY 2017 to further enhance its cybersecurity program, which will include designing and implementing an Enterprise Security Operations Center to include security data analytics, log-based forensics, and intrusion detection and prevention systems. These capabilities will provide automated real-time risk and threat analysis of Labor's environment and will be readily available to all levels of Labor staff, including Labor executives. This will enable Labor to execute timely and proactive countermeasures to prevent exposure of Labor information and information systems.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 2: Defined  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 5: Optimized

Labor has defined responsibilities and policies for Identify, Protect, and Recover. The agency is also in the process of implementing technologies needed for Vulnerability Management, security information and event management, and asset and device management. Despite this progress, Labor continues to rely on manual and procedural methods in instances where automation would be more effective, and it retains deficiencies in its Risk Management, Contractor Systems, Identity Control and Access Management, Configuration Management, and Contingency Planning program areas. During FY 2016, the Office of Inspector General's (OIG) review of 23 departmental information systems identified a total of 82 control deficiencies, 62 deficiencies in financial systems and 20 deficiencies in non-financial systems.

Many of these issues have recurred over a number of years and have been reported by OIG multiple times. Central to addressing these issues is realigning the organization to provide the Chief Information Officer the needed independence and authority to implement corrective actions.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 99%	100%	58%
Software Asset Management	✓ 96%	100%	98%
Vulnerability Management	✓ 99%	100%	95%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 93%	100%	98%
Privileged User PIV Implementation	✓ 96%	100%	100%
Anti-Phishing Defenses	✓ 6	6	6
Malware Defenses	✓ 3	3	3
Other Defenses	✓ 2	2	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 293

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	60
External/Removable Media	0
Impersonation/Spoofing	1
Improper Usage	4
Loss or Theft of Equipment	92
Web	7
Other	118
Multiple Attack vectors	11



# Cybersecurity Performance Summary

Department of State

## Chief Information Officer Assessment

As defined in the Department of State's (State) Cyberstrategy and Framework, the mission of the cyber program is to "Establish and continually refine a state-of-the-art cybersecurity program to enable innovation and effectively safeguard and support the Department's global information assets and operations and those of the foreign affairs community." State is creating an information security risk management strategy, and will monitor information security risk at all levels by procuring a Governance, Risk Management, and Compliance tool to improve Authority to Operate (ATO) and Plans of Action and Milestones management. State has also established the Cloud Computer Governance Board to ensure appropriate and authorized use of cloud services. State improved identity and authentication management by requiring all users of workstations to use two-factor authentication to access those networks. This effort will expand to include deployment of privileged account management tools that limit the availability of those accounts. State continues to leverage the Continuous Diagnostics and Mitigation (CDM) program. State deployed a phishing awareness tool that tests and trains employees on phishing attacks. State established the Cybersecurity Integrity Center to assist in detecting anomalous behavior and to mitigate security issues on the network. State has implemented high availability and disaster recovery tests to maintain operations in the event of a disaster or outage. State continues to improve its cybersecurity posture and provide transparency across the agency.

## Inspector General Assessment

- Identify** Level 1: Ad-Hoc
- Protect** Level 1: Ad-Hoc
- Detect** Level 1: Ad-Hoc
- Respond** Level 1: Ad-Hoc
- Recover** Level 1: Ad-Hoc

The Office of the Inspector General (OIG) found that State did not have an effective organization-wide information security program, guided by risk-based decision making, to identify, protect, detect, respond, and recover from information security risks, which is evidenced by the control weaknesses identified in the FISMA metric domains. The reason State does not have an effective organization-wide information security program is because it did not prioritize resources to fully develop and implement an organization-wide risk management strategy and had not developed a timeline with specific milestones to achieve a fully developed and implemented information security risk management strategy since FY 2010. Without developing and implementing an effective organization-wide information security program, State cannot achieve its core mission.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	81%	81%	81%
Software Asset Management	✓ 98%	98%	98%
Vulnerability Management	82%	88%	88%
Secure Configuration Management	✓ 95%	99%	99%
Unprivileged User PIV Implementation	47%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	6	6
Malware Defenses	✓ 4	5	5
Other Defenses	✓ 3	4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,003

Attack Vector	Number of Incidents
Attrition	1
Email/Phishing	116
External/Removable Media	1
Impersonation/Spoofing	0
Improper Usage	240
Loss or Theft of Equipment	2
Web	89
Other	543
Multiple Attack vectors	11



# Cybersecurity Performance Summary

Department of the Interior

## Chief Information Officer Assessment

In FY 2016, Department of the Interior (Interior) developed and formally released the Interior Cybersecurity Strategy to better adhere to the NIST Cybersecurity Framework and align its cybersecurity strategy with that of the OMB M-16-04, the Cybersecurity Strategy and Implementation Plan. This has enabled Interior to focus on the high priorities defined within the CAP Goal targets, and the objectives defined within the Cybersecurity Strategy and Implementation Plan. In FY 2016, Interior made improvements in the following areas:

- Reducing the number of Privileged Users across the entire Department,
- Enforcing Strong Authentication for 99% of privileged users with the goal of reaching 100% (no exceptions) during FY 2017,
- Enforcing Strong Authentication for 89% of unprivileged users (exceeding the 85% target),
- Completing a High Value Asset inventory and review,
- Continuing the deployment of Continuous Diagnostics and Mitigation (CDM) tools, and
- Addressing Indicators of Compromise 100% of bureau and office systems.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 2: Defined

An independent assessment was conducted over the Interior's information security program, to include its Bureaus and Offices. A representative sample of 13 of 122 operational information systems were evaluated. Interior is in the process of updating information technology (IT) security policies and procedures to be aligned with NIST Special Publication 800-53 Revision 4. More specifically, the Interior IT Security Control Standards and Incident Response procedures have not been formalized. The NIST Cybersecurity Framework Functions of Identify, Protect, Detect, Respond, and Recover were identified as not effective. More specifically, improvements are needed in risk management, contractor systems, configuration management, identity and access management, information security continuous monitoring, incident response, and contingency planning.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	46%	46%	23%
Software Asset Management	57%	57%	68%
Vulnerability Management	68%	68%	83%
Secure Configuration Management	✓ 99%	99%	77%
Unprivileged User PIV Implementation	✓ 96%	96%	89%
Privileged User PIV Implementation	✓ 100%	100%	99%
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 2	2	5
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 310

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	71
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	26
Loss or Theft of Equipment	22
Web	49
Other	133
Multiple Attack vectors	9



# Cybersecurity Performance Summary

Department of the Treasury

## Chief Information Officer Assessment

Department of the Treasury (Treasury) attained a number of milestones in FY 2016, including:

- Met or exceeded administration CAP Goal targets for Secure Authentication and Anti-Phishing and Malware Defense,
- Mandated bureau use of Blanket Purchase Agreements issued by the General Services Administration for procurement of Identity Protection Services in the event of a breach of personally identifiable information,
- Launched an enterprise capability enabling all Treasury bureaus to conduct phishing exercises to test response to receipt of potentially malicious email.

Treasury remains committed to providing appropriate protection of its critical information and systems. The FY 2016 independent FISMA audit indicates that we continue to maintain our information security programs and practices. The recommendations issued by the Inspector General (IG) will help guide improvements in the coming year. Treasury is also engaged with Federal partners to deploy Phase 1 of the Continuous Diagnostics and Mitigation (CDM) program across the Treasury enterprise. Throughout FY 2017, Treasury will introduce new information technology (IT) management capabilities to provide near real-time awareness of enterprise-wide cybersecurity posture

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 2: Defined
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 3: Consistently Implemented

Treasury's information security programs and practices for its unclassified systems were established and maintained for the five cybersecurity functions and the eight FISMA program areas. There were six deficiencies within three of the cybersecurity functions and four of the FISMA program areas. For Internal Revenue Services (IRS) unclassified systems, Treasury Inspector General for Tax Administration (TIGTA) reported that IRS's information security program generally aligned with applicable FISMA, OMB, and NIST requirements and guidance. Due to program attributes not yet implemented, TIGTA found that three security program areas failed to meet FISMA requirements.

Treasury established and maintained its information security program and practices for collateral national security systems for the five cybersecurity functions and eight FISMA program areas. Five deficiencies were identified within two of the cybersecurity functions and four of the FISMA program areas.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	83%	83%	86%
Software Asset Management	91%	91%	94%
Vulnerability Management	✓ 98%	98%	100%
Secure Configuration Management	✓ 99%	99%	98%
Unprivileged User PIV Implementation	✓ 98%	98%	97%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	4	6
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 4	4	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 602

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	10
External/Removable Media	10
Impersonation/Spoofing	0
Improper Usage	15
Loss or Theft of Equipment	315
Web	22
Other	226
Multiple Attack vectors	4



# Cybersecurity Performance Summary

Department of Transportation

## Chief Information Officer Assessment

Department of Transportation's (DOT) Office of the Chief Information Officer (OCIO) devoted significant resources towards the following efforts in FY 2016: completing actions on 19 FISMA audit recommendations issued by the Office of Inspector General (OIG); meeting or exceeding CAP Goal targets for hardware asset management, strong authentication, and anti-phishing and malware defense; implementing EINSTEIN 3 Accelerated (E<sup>3</sup>A) protective capabilities at DOT headquarters which services approximately 20,000 personnel and more than 130 systems; executing phishing exercises for 68,000 personnel, achieving a 91% reduction in click-through rates; completing an assessment of wired and wireless networks which resulted in improved visibility into network infrastructure by 18%, and enabled remediation of more than 72% of serious configuration vulnerabilities within 30 days of first identification; deploying and authorizing a modernized agency personal security system modeled after solutions deployed in other agencies, and using Personal Identity Verification (PIV) for authentication; integrating cybersecurity reviews into IT spend reviews required by Federal Information Technology Acquisition Reform Act (FITARA); increasing deployment of Continuous Diagnostics and Mitigation (CDM) Phase 1 capabilities, and kickoff for Phase 2 capabilities; and recruiting a Deputy Chief Information Security Officer (CISO) and three additional cyber personnel, doubling the size of the DOT CISO Office.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 2: Defined

OIG reviewed a statistical sample of 75 systems, 70 systems that had expired authorizations to operate (ATO), and enterprise wide security activities, such as information security continuous monitoring. OIG placed most emphasis on two DOT components which control the three largest, key networks: the Federal Aviation Administration (FAA) and Office of the Secretary of Transportation (OST). OIG determined that the maturity level for the information security program is "Level 2 – Defined" across three Security Functions: Identify, Protect, and Recover; and "Level 1 – Ad Hoc" for the remaining two Security Functions: Detect and Respond. OIG found numerous deficiencies across all domains in FAA and OST, and other components, in these areas: security authorization; risk management; weakness monitoring; user identity and access management; security training; information security continuous monitoring; incident handling and reporting; and contingency planning and testing. DOT needs to perform better across all domains. OIG concludes that although DOT continues to make improvements, its cybersecurity program remains ineffective.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 99%	99%	99%
Software Asset Management	90%	90%	90%
Vulnerability Management	30%	86%	86%
Secure Configuration Management	23%	98%	98%
Unprivileged User PIV Implementation	✓ 97%	97%	97%
Privileged User PIV Implementation	✓ 98%	98%	98%
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 192

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	8
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	7
Loss or Theft of Equipment	9
Web	5
Other	160
Multiple Attack vectors	3



# Cybersecurity Performance Summary

Department of Veterans Affairs

## Chief Information Officer Assessment

Department of Veterans Affairs (VA) has an effective information security program and remains committed to making additional progress in securing its information technology (IT) infrastructure as expeditiously as possible. VA has achieved a significant portion of its CAP Goal targets, and while there is still work to do, the Department will make significant improvements in the coming months. VA has already met the Vulnerability, Secure Configuration Management, Anti-Phishing Defense, Malware Defense, and Other Defenses CAP Goal targets. In addition, VA has dramatically increased efforts to technically force users to log on with Personal Identity Verification (PIV) cards, exceeding the goal established for FY 2016. Improvement in continuous monitoring via implementation of the Continuous Diagnostics Monitoring (CDM) Program coupled with VA's Enterprise Cybersecurity Strategy initiatives, will continue to strengthen VA's dedication to information security and the Cybersecurity CAP Goals. In FY 2016 VA successfully deployed new, FedRAMP-approved cloud services.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

As noted in prior years, VA continues to have weaknesses in Configuration Management, Access Controls, Security Management, and Contingency Planning Controls designed to protect mission-critical systems from unauthorized access, alteration, or destruction. The Office of the Inspector General (OIG) continues to identify significant technical weaknesses in databases, servers, and network devices that support transmitting financial and sensitive information between VA's medical centers, regional offices, and data centers. Furthermore, OIG continues to see information system security deficiencies similar in type and risk level to OIG findings in prior years and an overall inconsistent implementation of the security program. In FY 2016, VA established and implemented an effective security and privacy training program. VA is still updating and improving its Incident Response program to ensure staff are trained to appropriately identify and measure the metrics necessary to ensure the program's effectiveness. While VA has identified some areas for improvement, VA has implemented an effective contingency planning program.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	0%	22%
Software Asset Management	0%	5%
Vulnerability Management	49%	96%
Secure Configuration Management	✓ 100%	✓ 99%
Unprivileged User PIV Implementation	80%	81%
Privileged User PIV Implementation	✓ 100%	✓ 100%
Anti-Phishing Defenses	✓ 6	✓ 5
Malware Defenses	2	✓ 3
Other Defenses	✓ 2	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 2,808

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	731
External/Removable Media	49
Impersonation/Spoofing	17
Improper Usage	53
Loss or Theft of Equipment	419
Web	1,015
Other	455
Multiple Attack vectors	69



# Cybersecurity Performance Summary

Election Assistance Commission

## Chief Information Officer Assessment

The Election Assistance Commission (EAC) system security plan was recently audited, and it was found that EAC generally complied with FISMA requirements. Two recommendations were provided that will further strengthen EAC's information security program, which the agency has already begun to implement.

In FY 2016, EAC met six out of nine CAP Goal capabilities areas, including Software Asset Management, Vulnerability Management, Privileged User PIV Implementation, Anti-Phishing Defenses, Malware Defenses, and Other Defenses. EAC did not meet the CAP Goal metrics for Hardware Asset Management, Secure Configuration Management, and Unprivileged User PIV Implementation capability areas.

## Inspector General Assessment

**Identify** Level 5: Optimized  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 5: Optimized

The EAC Office of the Inspector General (OIG) conducted an independent audit of its compliance with FISMA and related information security policies, procedures, standards, and guidelines. The audit included assessing EAC's effort to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the EAC. The audit found that EAC generally complied with FISMA requirements by implementing 56 of 60 security controls selected for testing; however weaknesses were noted in mitigating network vulnerabilities, and implementing controls surrounding audit logging and monitoring. The audit report makes two recommendations to assist EAC in strengthening its information security program, which were submitted to the EAC Chairman. Further details can be found in in the report (I-PA-EAC-02-16).

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Capability Area	✓ CAP Goal Met	2015	2016
Hardware Asset Management	85%	0%	0%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	93%	0%
Unprivileged User PIV Implementation	✓ 100%	0%	0%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	3	7	7
Malware Defenses	4	5	5
Other Defenses	3	4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Environmental Protection Agency

## Chief Information Officer Assessment

The Environmental Protection Agency (EPA) is diligently working to implement and maintain controls and processes that ensure information assets are protected in a manner consistent with the magnitude of harm that may result from the loss, misuse, or unauthorized access of information. In FY 2016, EPA made significant progress towards meeting the Administration's Cybersecurity CAP Goal targets. EPA met four out of nine CAP Goal capabilities, including Secure Configuration Management, Unprivileged User PIV Implementation, Privileged User PIV Implementation, and Anti-Phishing Defenses. EPA will continue to work aggressively in FY 2017 towards meeting CAP goals and mitigating weaknesses. EPA will implement Continuous Diagnostics and Mitigation Phase I capabilities that will significantly help achieve Vulnerability and Hardware and Software Asset Management goals. EPA will continue with cybersecurity projects started and planned to achieve Malware and Other Defenses goals and mitigate weaknesses. For example, EPA will continue with improvements made in the Role Based Training Program, expanding it to senior executives and system security officers and extend credentialing requirements to more roles. The CIO's office will align security practitioners and processes to maximize the use of specialized knowledge, skills and abilities and improve systems' security. EPA will pilot a cross-agency security team model to operate vulnerability scanning tools and processes for the agency. EPA will continue to actively manage Plans of Action and Milestones, continuously reviewing to ensure mitigations are properly planned and implemented for all identified weaknesses.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	2%	0	0
Software Asset Management	67%	67%	67%
Vulnerability Management	0%	0%	0%
Secure Configuration Management	✓ 98%	98%	98%
Unprivileged User PIV Implementation	✓ 97%	97%	97%
Privileged User PIV Implementation	✓ 99%	99%	99%
Anti-Phishing Defenses	4	4	5
Malware Defenses	0	0	2
Other Defenses	0	0	1

## Inspector General Assessment

- Identify**    Level 3: Consistently Implemented
- Protect**    Level 3: Consistently Implemented
- Detect**    Level 2: Defined
- Respond**    Level 3: Consistently Implemented
- Recover**    Level 3: Consistently Implemented

EPA's information security function areas did not meet the defined requirements to be considered effective. The Office of the Inspector General (OIG) assessed the five Cybersecurity Framework function areas and the corresponding metric domains as specified by the FY 2016 Inspector General (IG) FISMA reporting metrics. The EPA does not have separate reporting bureaus or departments, and our analysis covers the agency's enterprise-wide information security program. The OIG evaluated each security function area using the maturity model as a tool to summarize the status of an agency's information security program. The table above depicts EPA's maturity models for each security function area. EPA must meet all requirements of that level before progressing to the next level within the maturity model. Based on the metrics, EPA would need to achieve Level 4 Managed and Measurable for a function area to be considered effective. As such, more work is needed by EPA to achieve managed and measurable information security function areas to manage cyber risks. Specifically, EPA should take steps to strengthen its processes surrounding: Risk Management; Contractor Systems; Identity and Access Management; Security and Privacy Training; and Incident Response.

### US-CERT Incidents by Attack vector

Total Number of Incidents: 221

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	22
External/Removable Media	3
Impersonation/Spoofing	7
Improper Usage	9
Loss or Theft of Equipment	11
Web	153
Other	16
Multiple Attack vectors	0





# Cybersecurity Performance Summary

Equal Employment Opportunity Commission

## Chief Information Officer Assessment

While a small, independent agency, the Equal Employment Opportunity Commission (EEOC) complies with the core components of FISMA, including: prioritizing risks into plans of actions and milestones; monitoring and remediating vulnerabilities; incorporating security and privacy clauses into contracts; completing incident response and disaster recovery testing; and implementing an Information Security Continuous Monitoring program.

In FY 2016, EEOC met four out of nine CAP Goal capabilities, including Software Asset Management, Secure Configuration Management, Malware Defense, and Other Defenses. Of particular note, EEOC increased the percentage of email messages processed by systems that quarantine or otherwise block suspected malicious traffic, which attributed to meeting the Other Defenses capability in FY 2016.

EEOC is presently transitioning to Microsoft Active Directory (AD) which is configured to support PIV logical access. AD and required PIV use is expected to be deployed to privileged and unprivileged users in Quarter 4 FY 2017. All government furnished equipment workstations are configured with PIV readers.

## Independent Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 3: Consistently Implemented
<b>Recover</b>	Level 5: Optimized

An independent evaluation was conducted regarding the effectiveness and efficiency of the EEOC information security program and practices.

The FISMA independent evaluation methodology included: 1) Interviews with EEOC management and staff; 2) Review of legal and regulatory requirements; and 3) Review of documentation relating to EEOC's information security program.

The independent evaluation found that EEOC continues to make positive strides in addressing information security weaknesses and improving the effectiveness and efficiency of its information security program. EEOC has consistently implemented controls regarding: Risk Management, Contractor System Protection, Configuration Management, Identity and Access Management, Security and Privacy Training, and Incident Response. EEOC has optimized its procedures regarding Contingency Planning. However, the agency still faces challenges to consistently implementing information security requirements regarding Information System Continuous Monitoring.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	6%	6%	18%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%		
Privileged User PIV Implementation	0%		
Anti-Phishing Defenses	4	4	2
Malware Defenses	✓ 3	3	3
Other Defenses	1	1	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 20

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	3
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	2
Other	14
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Export-Import Bank of the United States

## Chief Information Officer Assessment

The Export-Import Bank of the United States' (EXIM) information security program successfully identifies system inventory assets with a high degree of accuracy. Programs for protection of agency assets are satisfactory; however a comprehensive solution for testing phishing attempts is among the planned activities for further protection of EXIM's on-premises and cloud service assets in the coming year. Likewise, while its network defense efforts are steadily increasing, the agency plans to upgrade its abilities in FY 2017 to detect exfiltration attempts, and attempts to access large volumes of data, and effectively investigate such incidents. EXIM's incident response capabilities continue to be tested and upgraded to meet new challenges, as will its efforts to effectively test and evaluate IR policies and procedures. This will ensure roles and responsibilities are both understood and come as second nature by those tasked with implementation. The state of EXIM's recovery plan is effective.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 2: Defined  
**Respond** Level 2: Defined  
**Recover** Level 5: Optimized

To determine whether EXIM Bank developed and implemented effective information security programs and practices as required by FISMA, we performed a high-level review of each of the Bank's four major systems and performed detailed steps, as outlined in the DHS FY 2016 Inspector General FISMA Reporting Metrics, to evaluate EXIM Bank's information security policies, procedures, and practices. We noted that EXIM Bank addressed several of the challenges identified during previous fiscal year FISMA audits, however, when evaluating EXIM Bank's information security program against the DHS FY 2016 IG FISMA metrics, a five-level maturity model scale, we found that only one of the five NIST Cybersecurity Framework areas, the Recover domain, was effectively implemented consistent with FISMA requirements and applicable DHS and NIST guidelines. The remaining framework areas - Identify, Protect, Detect, and Respond – were not effectively implemented.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 95%	100%	100%
Software Asset Management	0%	0%	0%
Vulnerability Management	51%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 97%	97%	97%
Privileged User PIV Implementation	81%	100%	100%
Anti-Phishing Defenses	3	6	6
Malware Defenses	0	4	4
Other Defenses	1	2	2

### US-CERT Incidents by Attack vector

Total Number of Incidents: 4

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	3
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Farm Credit Administration

## Chief Information Officer Assessment

Farm Credit Administration (FCA) has a comprehensive information security program that is consistent with Federal guidelines. FCA continues to make improvements on an annual basis.

The CAP Goal metrics for Information Security Continuous Monitoring (ISCM) capability areas of Hardware Asset Management, Software Asset Management and Vulnerability Management were met at 100%. The ISCM capability area of Secure Configuration Management was not met due to a decrease in FY 2016. In 2016, FCA miscalculated, by 90, the total servers that are actually covered by a tool that audits compliance with a common security configuration baseline, resulting in a decrease in the percentage of assets covered. The CAP Goal metrics for Identity Credential and Access Management were met at 100%, and CAP Goal metrics were met for the areas of Anti-Phishing Defenses and Other Defenses capability areas. The CAP Goal target for Malware Defenses was not met, although progress was made from FY 2015.

FCA continues to mature its continuous monitoring efforts and privacy program to maximize protection of FCA information. Automated capabilities will allow FCA staff to focus on program development and to keep pace with government-wide security and privacy initiatives. As with many small agencies, tools and assistance from the DHS programs are key components in achieving information security goals.

## Inspector General Assessment

- Identify** Level 4: Managed and Measureable
- Protect** Level 4: Managed and Measureable
- Detect** Level 2: Defined
- Respond** Level 2: Defined
- Recover** Level 5: Optimized

FCA has an information security program that continues to mature. FCA needs to define ISCM processes that will be utilized and improve documentation of its ISCM and incident response programs. Additionally, FCA needs to identify and define performance measures that will be used to assess the effectiveness of its ISCM and incident response programs. Although FCA's information security program is not ranked "Effective" based on the DHS's scoring methodology, the Office of the Inspector General (OIG) did not make any recommendations because FCA continues to identify areas to strengthen and improve information security.

FCA is a single program Agency with eight mission critical systems and major applications. The scope of this evaluation covered FCA's Agency-owned and contractor-operated information systems of record as of September 30, 2016.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	0%	0%	0%
Secure Configuration Management	✓ 100%	100%	76%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	5	5
Malware Defenses	1	2	2
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 63

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	18
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	10
Web	1
Other	32
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Federal Communications Commission

## Chief Information Officer Assessment

Federal Communications Commission (FCC) is committed to remediating information technology (IT) control deficiencies. The Commission's IT team worked diligently throughout FY 2016 to make improvements and to resolve audit findings from previous audits. The auditors recognized FCC has improved its overall information security program and its compliance with the FISMA and related guidance. In FY 2016, the Chief Information Officer led a team focused on improving the Commission's security posture. This initiative and the work completed in prior fiscal years reduced the overall Commission's FISMA findings by 64% from FY 2012. The Commission is working diligently to resolve the remaining 29 findings.

In addition to its FISMA findings reduction efforts, the Commission has continued to improve its overall information security program. The Commission improved or maintained its security posture in five of the eight metric domains. Also, the Commission made the most significant progress qualitatively in the area of risk management with the establishment of a formal IT risk management and governance program. In FY 2016, the Commission will continue to address all weaknesses in its information systems and data stores.

## Inspector General Assessment

- Identify** Level 1: Ad-Hoc
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 3: Consistently Implemented
- Recover** Level 2: Defined

FCC has improved its overall information security program since the FY 2015 evaluation, most notably in establishing a formal IT risk management and governance program. Although FCC has made progress, the Inspector General's (IG) evaluation assessed the FCC information security program as "Not Effective" in seven of the eight FISMA metric domains and "Effective" in the Security and Privacy Training domain. FCC management should prioritize and direct attention to four domains, specifically information security continuous monitoring (ISCM), identity and access management, risk management, and contractor systems. The IG evaluation concluded that the FCC's information security program was not in compliance with FISMA legislation, OMB guidance, and applicable NIST Special Publications as of September 30, 2016.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	0%	0%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	7%	7%	99%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	0%
Anti-Phishing Defenses	✓ 6	6	7
Malware Defenses	✓ 3	3	5
Other Defenses	✓ 1	1	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 74

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	3
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	34
Web	2
Other	33
Multiple Attack vectors	2



# Cybersecurity Performance Summary

Federal Deposit Insurance Corporation

## Chief Information Officer Assessment

The Federal Deposit Insurance Corporation (FDIC) has established a number of information security program controls and practices that are generally consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. Further, FDIC updates its practices to keep up-to-date with the ever-evolving security landscape and is currently consolidating its information security guidance to be more straightforward and easier to update going forward. FDIC maintains a robust program for self-identifying security weaknesses and correspondingly maintains a risk-focused approach to Plans of Action and Milestones to address these weaknesses. This has resulted in risk reduction for FDIC. There were several questions in this year's metrics that relied on the implementation of particular solutions that FDIC does not use; however, FDIC has implemented equivalent compensating controls. FDIC undertook action to strengthen its security program during the FY 2016 reporting period. Nonetheless, there are still some areas in which it can improve its information security program and practices, and FDIC has worked on several initiatives to address these improvements. For example, after the annual reporting period but by the end of December 2016, FDIC upgraded access controls through mandatory PIV logical access, with limited exceptions. Additionally, FDIC has implemented a solution for greater management of cyber incident response.

## Inspector General Assessment

- Identify** Level 3: Consistently Implemented
- Protect** Level 3: Consistently Implemented
- Detect** Level 2: Defined
- Respond** Level 1: Ad-Hoc
- Recover** Level 3: Consistently Implemented

The assessment covered key components of FDIC's information security program and selected security controls pertaining to four general support systems and an outsourced service provider. FDIC had 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 established policies in most security control areas reviewed; provided security awareness training to its users; and updated its security control framework to address current NIST guidance. However, weaknesses existed that impaired the effectiveness of FDIC's security program and placed the confidentiality, integrity, and availability of its systems and data at elevated risk. Weaknesses were identified in such areas as information security strategic planning, vulnerability scanning, the information security management program, baseline configurations, and vendor software (including patching). The assessment resulted in a series of recommendations to improve the effectiveness of FDIC's security program. FDIC was working to address all of the security weaknesses described in the report. A public Executive Summary of the assessment can be found at <http://www.fdicig.gov/>

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	89%	89%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	92%	92%	100%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	3%
Anti-Phishing Defenses	✓ 6	6	5
Malware Defenses	0	0	4
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 291

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	8
External/Removable Media	0
Impersonation/Spoofing	1
Improper Usage	139
Loss or Theft of Equipment	108
Web	13
Other	22
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Election Commission

## Chief Information Officer Assessment

Since the Federal Election Commission (FEC) is exempt from the FISMA and the E-Government Act, the Agency did not provide responses for portions of the report that derive from those statutes, including all sections of the Chief Information Officer Report.

## Independent Assessment

- Identify** Level 5: Optimized
- Protect** Level 5: Optimized
- Detect** Level 5: Optimized
- Respond** Level 5: Optimized
- Recover** Level 5: Optimized

The Office of General Counsel (OGC) concluded that the FEC is not included in the applicable definition of "agency" under FISMA or the E-Government Act, hence, the Agency did not provide responses for portions of the report, including all sections of the Inspector General (IG) Report. On advice from DHS, FEC standardized a single answer for the metrics since all questions must be answered and "NA" is not an accepted answer.

## CAP Goal Metrics

✓ CAP Goal Met ■ 2015 ■ 2016

Metric	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	0%
Vulnerability Management	0%	0%
Secure Configuration Management	0%	100%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	0	0
Malware Defenses	0	0
Other Defenses	0	0

## US-CERT Incidents by Attack vector

Total Number of Incidents: 105

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	5
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	10
Other	88
Multiple Attack vectors	2



# Cybersecurity Performance Summary

Federal Energy Regulatory Commission

## Chief Information Officer Assessment

The Federal Energy Regulatory Commission (FERC) is committed to maintaining a strong cybersecurity posture for its information systems and data, viewing it as a critical function to meet FERC's mission. In FY 2016, FERC continued to make a significant investment in establishing a cost-effective information security program that manages FERC's security risks. Some highlights from this FY include:

- Completed a comprehensive update of 26 FERC cybersecurity policies,
- Developed and leveraged a maturity model approach to measuring and managing 12 cyber functional security areas, and
- Implemented new Vulnerability Management processes and modernized information security tool sets to enhance cyber operations and situational awareness.

## Inspector General Assessment

**Identify** Level 5: Optimized  
**Protect** Level 5: Optimized  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 2: Defined  
**Recover** Level 5: Optimized

The Office of Inspector General (OIG) conducted its annual evaluation of the Commission's unclassified information security program to assess the effectiveness of unclassified information security policies, procedures, and practices within five information security functions: Identify, Protect, Detect, Respond, and Recover. The OIG determined that the Commission was effective in three of five information security functions (Identify, Protect, and Recover) but not effective in the remaining two information security functions (Detect and Respond). Specifically, OIG found that the Commission had consistently implemented security practices for the Detect security function (Level 3), while it had defined security practices for the Respond security function (Level 2).

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	92%
Software Asset Management	53%	69%	69%
Vulnerability Management	91%	100%	100%
Secure Configuration Management	✓ 99%	98%	98%
Unprivileged User PIV Implementation	✓ 100%	97%	97%
Privileged User PIV Implementation	49%	100%	100%
Anti-Phishing Defenses	3	4	4
Malware Defenses	✓ 4	2	2
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 5

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	5
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Housing Finance Agency

## Chief Information Officer Assessment

Based upon the CAP Goal Target metrics, Federal Housing Finance Agency (FHFA) continues to make improvements on an annual basis. For Information Security Continuous Monitoring (ISCM), FHFA met its CAP Goals Metrics in the areas of Hardware Asset Management and Vulnerability Management. The CAP Goals for the ISCM areas of Software Asset Management and Secure Configuration Management were not met, although both increased between FY 2015 and FY 2016. The CAP Goal Metrics for Identity Credential and Access Management and Anti-Phishing and Malware Defenses were met for FY 2016.

## Independent Assessment

- Identify** Level 5: Optimized
- Protect** Level 5: Optimized
- Detect** Level 4: Managed and Measureable
- Respond** Level 4: Managed and Measureable
- Recover** Level 5: Optimized

To meet FISMA requirements with respect to FHFA, the agency contracted with an independent auditor to conduct the FY 2016 independent evaluation of FHFA's information security program and practices as a performance audit under Generally Accepted Government Auditing Standards. The auditors for FHFA concluded that FHFA's information security program was compliant with FISMA and applicable OMB guidance and that sampled security controls from NIST Special Publication 800-53 demonstrated operating effectiveness.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	9%	9%	100%
Software Asset Management	11%	11%	16%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	74%	74%	93%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	2	2	5
Malware Defenses	2	2	3
Other Defenses	3	3	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 11

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	6
Web	1
Other	3
Multiple Attack vectors	0





# Cybersecurity Performance Summary

Federal Labor Relations Authority

## Chief Information Officer Assessment

Federal Labor Relations Authority (FLRA) has a strong information security program. FLRA uses a combination of government staff time and contract support where possible to manage its CyberSecurity Program. In the current funding environment, where the FLRA – like many agencies -- must continue to innovate with less while meeting increased mission requirements and rising customer expectations, the FLRA continually looks to take advantage of evolving technologies and methodologies to accomplish its mission support functions more effectively and efficiently, while improving quality and flexibility. The key to the FLRA’s success in meeting these goals is the ability to collaborate across government and work together to leverage resources. This has allowed the FLRA to continue to update and make progress in accomplishing its established Plan of Action and Milestones (POA&Ms). For FY 2016, the FLRA met the CAP Goal Target metrics in all but two categories -- Hardware Asset Management and Unprivileged User PIV Implementation. Both categories are open POA&Ms, and are being actively managed under the agency POA&M processes. The FLRA has made significant progress in addressing outstanding IT security program weaknesses, and is confident that its program will continue to strengthen.

## Inspector General Assessment

- Identify** Level 3: Consistently Implemented
- Protect** Level 3: Consistently Implemented
- Detect** Level 4: Managed and Measureable
- Respond** Level 5: Optimized
- Recover** Level 5: Optimized

Overall, the FLRA has an effective information security program. They maximize their resources and provide a security posture that is sound. Incidentally, the last FISMA testing resulted in no new findings. Previously, they had 11 prior findings and were able to close 6 of the 11, whereas the remaining 5 are expected to be closed this year. FLRA has extensive policies and procedures, and extensive controls in place. FLRA has a robust security program with regular scanning, and a host of both physical and logical security controls.

Our evaluation includes the use of an external service provider to perform the annual FISMA audit over the various IT controls at the FLRA. NIST Special Publication 800-53 Revision 4 has nearly 200 controls for Moderate categorized systems (FIPS-199 categorization) and while FLRA attempts to comply with all of the controls; our external service provider makes a sample of those controls and assesses them for their operating effectiveness and design of control.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	79%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	4	6
Malware Defenses	2	2	4
Other Defenses	1	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	1
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Maritime Commission

## Chief Information Officer Assessment

The Federal Maritime Commission's (FMC) information system continuous monitoring (ISCM) strategy consists of a multi-tiered approach. FMC has implemented an enterprise solution to allow the agency to continuously manage risk and security compliance by providing information on the current state of all server and desktop systems. To identify known vulnerabilities on its servers, the agency uses a vulnerability scanner, which generates reports and classifies the vulnerabilities based on their severity, thus allowing for quick remediation. FMC has anti-virus technologies distributed throughout the agency's desktop and server environment to protect against malware. FMC also employs tools to monitor file activity and account behavior in order to prevent unauthorized access and report on account management and configuration.

FMC is a participant in the DHS's Continuous Diagnostics and Mitigation (CDM) Program. It is also a participant in the National Cybersecurity Assessment and Technical Services assessment process, which provides vulnerability scans of the agency's external interfaces for known and potentially new vulnerabilities.

## Inspector General Assessment

- Identify** Level 5: Optimized
- Protect** Level 3: Consistently Implemented
- Detect** Level 4: Managed and Measureable
- Respond** Level 5: Optimized
- Recover** Level 5: Optimized

FMC continues to make improvements on its information technology (IT) security although some weaknesses remain. The scope of the Inspector General (IG) evaluation focused on the FMC General Support Systems and Major Applications. The evaluation covered a sample of controls as listed in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 4.

In the Office of Inspector General's (OIG) FY 2016 evaluation of FMC's compliance with the FISMA, OIG concluded that FMC had effectively implemented six of the nine outstanding prior year recommendations. Further, OIG's FY 2016 FISMA evaluation report contained three recommendations to address these findings. Two of the three recommendations were implemented by FMC prior to the release of OIG's FY 2016 FISMA evaluation report. FMC management agreed to implement the one open recommendation, an improvement to the security awareness training program for agency contractors.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 95%	95%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 95%	95%	90%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	4	6
Malware Defenses	4	4	5
Other Defenses	2	2	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 3

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	3
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Mediation and Conciliation Service

## Chief Information Officer Assessment

The information security program at the Federal Mediation and Conciliation Service (FMCS) utilizes a blended approach and is still very much a work in progress. FMCS has many systems in place, but some are still manually oriented. We are in the process of implementing Managed Trusted Internet Protocol Services (MTIPS) based circuits from Verizon on the Networx contract. This is being implemented with the assistance of DHS and Verizon technicians as the first step to implementing Einstein 3 and other monitoring applications from DHS. We are implementing Office 365 in Microsoft's Government Cloud as our core desktop applications platform. We will be expanding our mobile device management via module to our F5 Secure Sockets Layer Virtual Private Network appliance. We are in the process developing a Windows 10 based policy to include a least necessary permission model that will be applied to our computer template to cover all end user computers supplied by the FMCS. Our plans are to have this fully implemented in FY 2017. These implementations will greatly enhance our continuous monitoring and secure environment capabilities and give us a fully effective security program that allows us to be flexible in our ability to respond to the ever changing electronic environment we live in.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 2: Defined

The information security program at the Federal Mediation and Conciliation Service (FMCS) utilizes a blended approach and is still very much a work in progress. FMCS has many systems in place, but some are still manually oriented. We are in the process of implementing MTIPS based circuits from Verizon on the Networx contract. This is being implemented with the assistance of DHS and Verizon technicians as the first step to implementing Einstein 3 and other monitoring applications from DHS. We are implementing Office 365 in Microsoft's Government Cloud as our core desktop applications platform. We will be expanding our mobile device management via module to our F5 Secure Sockets Layer Virtual Private Network appliance. We are in the process developing a Windows 10 based policy to include a least necessary permission model that will be applied to our computer template to cover all end user computers supplied by the FMCS. Our plans are to have this fully implemented in FY 2017. These implementations will greatly enhance our continuous monitoring and secure environment capabilities and give us a fully effective security program that allows us to be flexible in our ability to respond to the ever changing electronic environment we live in.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	0%
Vulnerability Management	0%	0%
Secure Configuration Management	✓ 100%	94%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	4
Malware Defenses	2	3
Other Defenses	1	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Retirement Thrift Investment Board

## Chief Information Officer Assessment

The Federal Retirement Thrift Investment Board (FRTIB) continues to review all facets of its information security program and has commissioned external support from key industry leaders to help assess gaps in its security posture. During the fiscal year, FRTIB conducted a penetration test with the DHS. FRTIB also participated in a compromise assessment conducted by an industry leader. Recommendations from these assessments were accepted and prioritized accordingly for remediation to enhance overall security posture. FRTIB started a number of initiatives to upgrade its systems and applications to improve the infrastructure and operating environment for its end users. FRTIB initiated a comprehensive review of its processes and procedures and has drafted and approved a number of new policies to help improve security and operational programs. FRTIB implemented an information technology (IT) Governance process to manage resources and assets required to maintain its current operations in alignment with FRTIB's Strategic Plan.

## Inspector General Assessment

**Identify** Level 1: Ad-Hoc  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 2: Defined

FRTIB conducted its first ever FISMA Inspector General (IG) assessment in 2016 due to FRTIB increased staffing. The scope of the FY 2016 FISMA IG assessment included 4 of the Agency's 19 systems in order to assess the agency's information security program and serve as a baseline for ongoing FISMA compliance and improvement. The independent assessment team made the following statement regarding the results of the audit, "Overall, in comparison with the Inspector General FISMA reporting metrics, FRTIB has significant opportunities to strengthen its information security program." Additionally the report states, "Despite the progress made to improve FRTIB's information security program over the past few years, opportunities to strengthen the program continue to exist." FRTIB received 26 recommendations from this assessment and are actively working to implement corrective actions.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	0%
Software Asset Management	0%	0%	0%
Vulnerability Management	✓ 100%	100%	88%
Secure Configuration Management	✓ 99%	99%	96%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	0%
Anti-Phishing Defenses	✓ 6	6	4
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 2	2	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 27

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	2
Web	0
Other	24
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Federal Trade Commission

## Chief Information Officer Assessment

Federal Trade Commission (FTC) has made considerable progress implementing additional cybersecurity controls over its information technology (IT) infrastructure in the past year. In particular, FTC implemented mandatory Homeland Security Presidential Directive -12 authentication for administrative logical access and initiated a phishing testing and training program. FTC's information security program continues to improve its posture through information system modernization and senior staff involvement. FTC's information system modernization projects include cloud-based service solutions to increase system availability and recovery options while facilitating automated continuous monitoring. FTC attained two new FISMA CAP goals in FY 2016 Privileged User PIV Implementation and Malware Defense. FTC is continuing to achieve additional FISMA CAP Goal targets by integrating them as requirements into the new service solutions.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 2: Defined

FTC has approximately 1,700 staff and support contractors, and leverages resources and technologies provided by DHS and General Services Administration.

The FY 2015 Office of Inspector General (OIG) FISMA evaluation showed that FTC security and privacy programs are robust, demonstrating their ability to protect FTC assets while undergoing organizational, physical, and technological change.

The OIG determined that the optimal maturity level that achieves cost-effective security based on FTC missions and risks is Level 3, Consistently Implemented, i.e., FTC will have an effective security program when all reporting metrics at Level 3 are completed. CyberScope scoring for FY 2016 shows FTC has met a number of metrics for Levels 4 and 5. Some metrics were not applicable or cost-effective for the FTC given its size, available resources, and mission.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	0%	0%	0%
Software Asset Management	26%	26%	26%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	7%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	4	4
Malware Defenses	✓ 3	2	3
Other Defenses	✓ 4	4	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 73

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	25
External/Removable Media	0
Impersonation/Spoofing	2
Improper Usage	9
Loss or Theft of Equipment	1
Web	1
Other	32
Multiple Attack vectors	3



# Cybersecurity Performance Summary

General Services Administration

## Chief Information Officer Assessment

General Services Administration (GSA) maintains a formalized program for information security management that is supported by a set of established policies, procedures, and processes to mitigate new and emerging threats and anticipate risks posed by new technologies. GSA continued to focus on implementing the cybersecurity capabilities that make up the Cybersecurity CAP Goal targets. GSA has met or exceeded the target values for all the CAP Goal targets.

GSA has a formal incident response program with promulgated policies, procedures and supporting processes based on the NIST Special Publication 800-61, United States Computer Emergency Readiness Team (US-CERT) Incident Reporting Guidelines, and the OMB Memorandum M-07-16. In the current FY, GSA further improved its incident handling capabilities, integrated into the DHS Automated Indicator Sharing program, adopted the updated US-CERT incident notification guidelines, and continued bi-annual tests of the agency incident response plan. GSA had no major incidents in FY 2016.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 4: Managed and Measureable  
**Recover** Level 3: Consistently Implemented

GSA has established an information security program for the eight FISMA metric domains as required by applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. However, while the security program has been established across GSA, the following five of eight FISMA program areas had 16 deficiencies: Risk Management, Contractor Systems, Configuration Management, Identity and access management, Contingency planning.

The GSA Office of the Inspector General (OIG) made 26 recommendations related to these control deficiencies that, if effectively addressed, should strengthen the respective information systems and GSA's information security program. The scope of the evaluation includes six information systems across GSA, which include six minor applications, five contractor systems, and entity-wide controls such as remote access, security awareness training, incident response, and continuous monitoring.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	73%	100%	100%
Software Asset Management	96%	100%	100%
Vulnerability Management	98%	100%	100%
Secure Configuration Management	95%	100%	100%
Unprivileged User PIV Implementation	99%	100%	100%
Privileged User PIV Implementation	100%	100%	100%
Anti-Phishing Defenses	6	5	5
Malware Defenses	3	3	3
Other Defenses	2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 665

Attack Vector	Number of Incidents
Attrition	5
Email/Phishing	174
External/Removable Media	0
Impersonation/Spoofing	2
Improper Usage	58
Loss or Theft of Equipment	335
Web	21
Other	70
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Institute of Museum and Library Services

## Chief Information Officer Assessment

The Institute of Museum and Library Services' (IMLS) mission is to serve as the leading source of quality data about the nation's people and economy. Protecting the systems that collect, process, and maintain that information is of critical importance. Information resources must include controls and safeguards to offset possible threats, and ensure data confidentiality, integrity, and availability. IMLS strives to ensure that data confidentiality and integrity are consistent with statutory requirements and ethical considerations, while meeting the need for availability.

IMLS met seven out of nine CAP Goal capability areas in FY 2016, which indicates that they have achieved an above average level of maturity with their incident handling processes. This is supported by noting only a single incident via US-CERT data.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 4: Managed and Measureable
<b>Recover</b>	Level 5: Optimized

IMLS's systems undergo ongoing monitoring performed by the Office of the Chief Information Officer. This monitoring consists of:

- The remediation of known weaknesses and unacceptable risks;
- Assessment of changes for impact to security risk and compliance posture (Impact Assessment);
- Vulnerability Assessment and Reporting;
- Ongoing monitoring of security events and audit logs;
- Ongoing selection and assessment of security controls, detecting ineffective controls;
- Updating of key documents (System Security Plan, Breach Notification Incident Policy, etc.); and
- Preparation of security status reports and obtaining ongoing authorization at least annually.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Hardware Asset Management	0%	✓	100%	
Software Asset Management	0%	✓	100%	
Vulnerability Management	0%	✓	100%	
Secure Configuration Management	0%	✓	100%	
Unprivileged User PIV Implementation	0%			
Privileged User PIV Implementation	0%			
Anti-Phishing Defenses	4	✓	7	
Malware Defenses	3	✓	5	
Other Defenses	2	✓	2	

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Inter-American Foundation

## Chief Information Officer Assessment

Inter-American Foundation (IAF) is a small government corporation that has invested significantly in its information technology (IT) program to comply with all Federal mandates and recommendations over the past five years.

IAF systems do not work with any classified information and are limited in their exposure to sensitive and personally identifiable information (PII). In FY 2016, IAF did not report a data breach, and systems were available 99.99% of the time.

Looking forward, IAF developed an FY17 mitigation plan with the specific goal of designing an effective security program. With respect to CAP Goal Metrics, IAF will implement or improve, as appropriate, asset management, multi-factor authentication, anti-phishing defense, and malware defense.

With respect to OIG's recommendations, we will update the security policy to align with NIST 800-53 revision 4 requirements. Controls will be designed, implemented, and/or optimized pertaining to vulnerability remediation, continuous auditing and monitoring, interconnection security agreements, continuity of operations testing, plan of action & milestones, and privacy. For FISMA systems, we will design and implement configuration and change management, security assessment and authorization, account management, and system security plan. Automation will be the desired approach to implementation.

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 1: Ad-Hoc

The Office of Inspector General contracted with an independent certified public accounting firm to conduct an audit to determine whether IAF implemented selected security controls for selected information systems in support of the FISMA. The firm tested IAF's implementation of selected controls outlined in NIST's Special Publication 800-53, Revision 4. The audit reviewed three systems.

Overall, IAF implemented 84 of 98 selected security controls for the 3 selected information systems. Although IAF generally had policies for its information security program, its implementation of those policies for 14 of the 98 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of the foundation's information and information systems. The audit made 13 recommendations to strengthen IAF's information security program, including remediation, continuous monitoring, baseline configuration, and system authorization controls. Detailed audit findings and recommendations to address identified weaknesses are outlined in Audit Report No. A-IAF-17-004-C, which can be found on the OIG's website.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	✓ 98%	98%
Vulnerability Management	86%	✓ 100%
Secure Configuration Management	✓ 100%	✓ 96%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	4	3
Malware Defenses	2	1
Other Defenses	1	✓ 2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	1
Multiple Attack vectors	0





# Cybersecurity Performance Summary

International Boundary and Water Commission

## Chief Information Officer Assessment

The International Boundary and Water Commission, United States and Mexico, US Section (USIBWC) consists of a general support system (GSS) and Supervisory Control and Data Acquisitions (SCADA) operational system. All information security programs comply with laws and regulation established by the FISMA and standards prescribed by the OMB and the NIST.

USIBWC met all nine CAP Goals.

## Inspector General Assessment

- Identify** Level 5: Optimized
- Protect** Level 5: Optimized
- Detect** Level 2: Defined
- Respond** Level 2: Defined
- Recover** Level 5: Optimized

The Office of Inspector General (OIG) found that USIBWC generally implemented an information security program and related practices with effective security controls for risk management and contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response, and contingency planning for its GSS. The OIG further reviewed access controls and personnel security and found that USIBWC implemented effective security controls for these areas for the GSS. The OIG also found that USIBWC defined comprehensive policies, procedures, and strategies consistent with NIST and OMB requirements for its GSS. The program and activities for the GSS were consistently applied across the organization, and USIBWC used metrics to measure and manage the program and activities. The OIG did recommend that USIBWC implement encryption for its personally identifiable information (PII) stored on its network and incident response and detection for its SCADA systems, and issue a Systems of Records Notice that addresses privacy information collected.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 6	6	7
Malware Defenses	✓ 4	4	5
Other Defenses	✓ 2	2	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

International Trade Commission

## Chief Information Officer Assessment

The primary challenge facing the US International Trade Commission (ITC) to the operation and further development of its information security program is staffing. Of the five authorized full-time staff positions, only two are currently filled despite multiple rounds of hiring efforts. This shortage is exacerbated by increasing external compliance requirements and new sources of cyber-threats and vulnerabilities.

To mitigate these challenges ITC is investing heavily in agency cyber-defense technology, and leveraging the resources of the DHS, such as the Continuous Diagnostics and Mitigation (CDM) Program BPA, CDM as a Service, and the DHS Cyber Hygiene program.

Additionally ITC has acquired short-term contract labor to address privacy compliance and policy development issues.

In the ITC's assessment, this approach has resulted in an improvement to its cybersecurity posture when compared to prior years.

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 1: Ad-Hoc
<b>Recover</b>	Level 2: Defined

Daily attention to the four foundational, critical security controls remain the cornerstone of securing ITC's network. These controls are:

- 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.

ITC has plans to deploy new technologies to meet shifting priorities and goals, such as a new data center and the implementation of a portal to support work on miscellaneous tariff bills. New projects introduce new risks as the focus moves from maintenance operations to developing and deploying new systems.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	59%	73%	73%
Vulnerability Management	89%	100%	100%
Secure Configuration Management	✓ 99%	98%	98%
Unprivileged User PIV Implementation	4%	79%	79%
Privileged User PIV Implementation	50%	100%	100%
Anti-Phishing Defenses	✓ 5	5	5
Malware Defenses	0	0	0
Other Defenses	0	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 9

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	3
Loss or Theft of Equipment	0
Web	3
Other	2
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Marine Mammal Commission

## Chief Information Officer Assessment

The Marine Mammal Commission (MMC) does not originate, receive, or store classified information. The Commission participates in the Managed Trusted Internet Protocol Service and EINSTEIN 3 Accelerated (E<sup>3</sup>A).

MMC met the CAP Goal capability areas for Vulnerability Management and Secure Configuration Management in FY 2016, but has not implemented Personal Identity Verification for its 26 employees.

MMC does not have an automated solution for hardware or software asset management, but manages inventory through a commercial-off-the-shelf electronic spreadsheet program.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for MMC was not performed for FY 2016 and this section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of the Inspector General (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 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	NA	0%
Software Asset Management	NA	0%
Vulnerability Management	✓ 100%	100%
Secure Configuration Management	✓ 100%	100%
Unprivileged User PIV Implementation	NA	0%
Privileged User PIV Implementation	NA	0%
Anti-Phishing Defenses	✓ 5	5
Malware Defenses	✓ 5	5
Other Defenses	✓ 4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Merit Systems Protection Board

## Chief Information Officer Assessment

The Merit Systems Protection Board (MSPB) shows progress towards meeting the FISMA metrics and the status of information security policies, procedures, and practices. In FY 2016, MSPB conducted an opportunity assessment of all Networkx enterprise vendors and selected a preferred provider for the Managed Trusted Internet Protocol Service (MTIPS). In September 2016, MSPB entered into updated agreements with the Office of Cybersecurity and Communications, DHS, relating to the deployment of EINSTEIN 3 Accelerated (E<sup>3</sup>A) cybersecurity capabilities. MSPB also signed an authorization letter with the MTIPS provider to comply and cooperate with DHS in deploying E<sup>3</sup>A on its network and MTIPS circuits. During FY 2016, MSPB met the Vulnerability Management, Software Asset Management, and Anti-Phishing Defense Cross-Agency Priority (CAP) Goal capability areas.

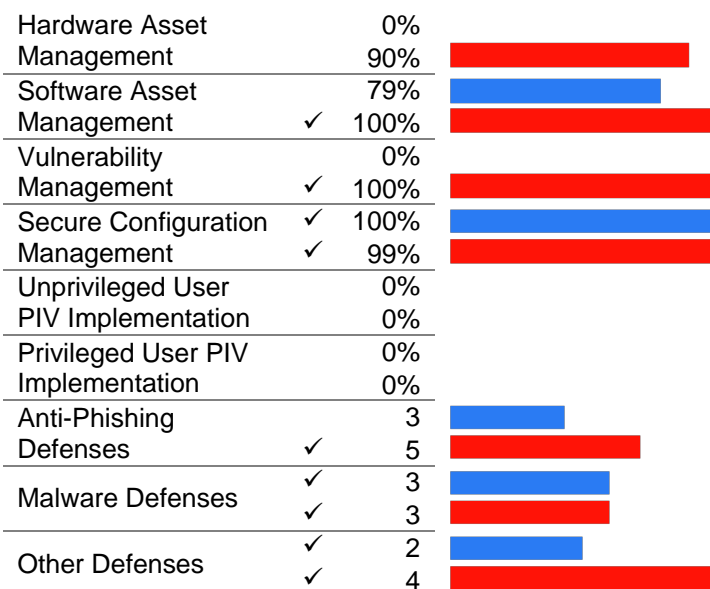
## Independent Assessment

**Identify** Level 2: Defined  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 5: Optimized

An independent evaluation of the status of the FISMA program for MSPB was not performed for FY 2016 and this section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of the Inspector General (OIG) appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. MSPB should explore contracting with an independent assessor in FY 2017.

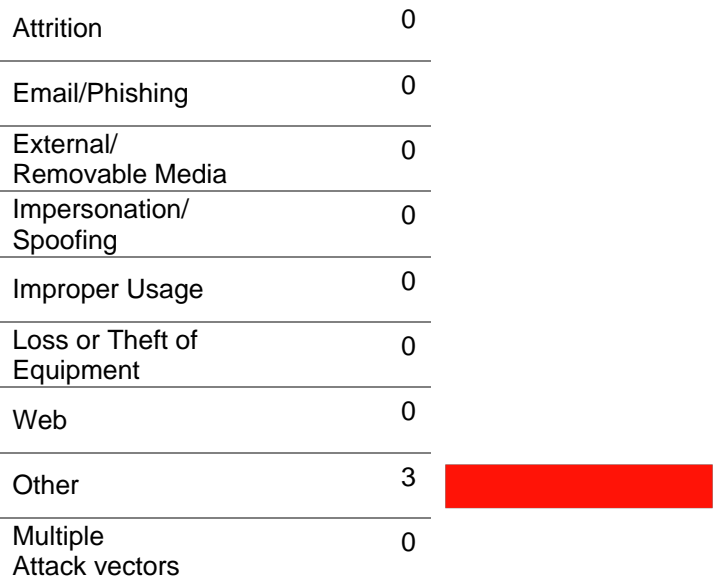
## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 3





# Cybersecurity Performance Summary

Millennium Challenge Corporation

## Chief Information Officer Assessment

The Millennium Challenge Corporation (MCC) has improved on its Cross-Agency Priority Goals by implementing a whitelisting program and a data management program. The whitelisting program allows execution of only authorized applications on information technology (IT) systems and the data management program provides greater visibility into insider threats or other malicious activities. In addition, MCC is on target to implement a network access control appliance that will improve the IT baseline. Lastly, MCC remains on target to implement multi-factor authentication to reach Homeland Security Presidential Directive-12 compliance on the network and on the agency's applications.

## Inspector General Assessment

**Identify** Level 4: Managed and Measureable  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 5: Optimized

The Office of Inspector General (OIG) contracted with an independent certified public accounting firm to conduct an audit to determine whether MCC implemented certain security controls for selected information systems in support of the FISMA. The firm tested MCC's implementation of selected controls outlined in NIST Special Publication 800-53, Revision 4. The audit reviewed five systems.

Overall, MCC implemented 85 of 102 selected security controls for the five selected information systems in support of FISMA. Although MCC had policies for its information security program, its implementation of those policies was not always fully effective. Specifically, MCC did not implement 17 controls designed to preserve the confidentiality, integrity, and availability of the Corporation's information and information systems. The audit made nine recommendations to strengthen MCC's information security program, including baseline configurations, access controls, physical and environmental controls, and physical security. Detailed audit findings and recommendations to address identified weaknesses are outlined in Audit Report No. A-MCC-17-003-C, which can be found on the OIG's website.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	0%
Software Asset Management	0%	34%	0%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	0%
Privileged User PIV Implementation	0%	0%	0%
Anti-Phishing Defenses	4	5	5
Malware Defenses	1	0	0
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 24

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	1
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	13
Web	2
Other	7
Multiple Attack vectors	0

# Cybersecurity Performance Summary

Morris K. Udall Foundation

## Chief Information Officer Assessment

The Morris K. Udall Foundation (MKUSENEP) is a micro agency with about 25 people on staff. While its resources are limited in both staff and budget, the agency strives to maintain a strong cybersecurity stance. For instance, firewall protection at the edge of the agency’s network provides MKUSENEP access controls and security services such as content filtering, gateway anti-virus, intrusion prevention, and anti-spyware. All workstations are protected with anti-virus software and agency-defined security policies in place. MKUSENEP’s users also receive annual cybersecurity training, and its network is scanned each month by DHS Cyber Hygiene, which identifies security gaps, if any. MKUSENEP is currently working on implementing DHS EINSTEIN 3 Accelerated (E<sup>3</sup>A), which should greatly enhance the cybersecurity stance once completed.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for MKUSENEP was not performed for FY 2016 and this section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of the Inspector General (OIG) appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. MKUSENEP will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Hardware Asset Management	0%	
Software Asset Management	0%	
Vulnerability Management	0%	
Secure Configuration Management	0% ✓ 100%	
Unprivileged User PIV Implementation	0%	
Privileged User PIV Implementation	0%	
Anti-Phishing Defenses	3 1	
Malware Defenses	1 1	
Other Defenses	0 ✓ 3	

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Aeronautics and Space Administration

## Chief Information Officer Assessment

In FY 2016, the National Aeronautics and Space Administration (NASA) focused efforts on modernizing information technology (IT) services and governance, leveraging Federal and private partnerships to improve security processes, and implementing leading enterprise security tools to reduce IT costs and risks. Specifically in FY 2016, NASA:

- Continued the phased procurement, design, and deployment of the Continuous Diagnostics and Mitigation (CDM) program tools and sensors to improve continuous monitoring and risk mitigation capabilities by FY 2017 Quarter (Q) 3;
- Expanded the capability to conduct quarterly anti-phishing attack exercises from 84% to 100% of NASA users to promote a culture of safe IT security practices;
- Continued to mitigate critical, high, and medium vulnerability findings in the weekly Cyber Hygiene report, resulting in a 25% reduction in aggregate risk posed by NASA's public-facing system;
- Deployed the infrastructure for an enterprise network access control solution to improve NASA's corporate network and IT asset security, with planned operational ability by FY 2017 Q3;
- Implemented an enterprise e-mail security and anti-phishing tool to reduce phishing incidents which increasingly account for the largest volume of cyber attacks at NASA.

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 1: Ad-Hoc
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 2: Defined
<b>Recover</b>	Level 2: Defined

Overall, NASA lacks an effective program in the five functions. NASA's scores in the Protect and Detect functions indicate a lack of formalized programs in those areas and a reactive—rather than proactive—performance posture. For the other three functions, scores indicate formalized programs in those areas but failure to consistently implement them agency-wide. NASA has several efforts underway in each of the functional areas to improve its information security program.

By implementing previous Office of Inspector General (OIG) audit recommendations and taking additional actions, NASA is working to improve its overall information security posture. Nevertheless, as indicated by the results of this review, information security remains a top management challenge for the Agency. Moving forward, NASA's information security program will continue to be examined both through focused audits of discrete issues and future FISMA reviews.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015 (%)	2016 (%)
Hardware Asset Management	0%	2%
Software Asset Management	2%	0%
Vulnerability Management	82%	89%
Secure Configuration Management	86%	84%
Unprivileged User PIV Implementation	76%	68%
Privileged User PIV Implementation	✓ 100%	✓ 100%
Anti-Phishing Defenses	3	✓ 6
Malware Defenses	2	✓ 3
Other Defenses	0	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,484

Attack Vector	Number of Incidents
Attrition	7
Email/Phishing	99
External/Removable Media	11
Impersonation/Spoofing	5
Improper Usage	141
Loss or Theft of Equipment	427
Web	678
Other	39
Multiple Attack vectors	77



# Cybersecurity Performance Summary

National Archives and Records Administration

## Chief Information Officer Assessment

The National Archives and Records Administration (NARA) continues to improve the effectiveness of its information security program to protect the confidentiality, integrity, and availability of NARA resources. In FY 2015 and FY 2016, the Agency declared a material weakness in internal controls over information technology (IT) security. Although more actions are needed, NARA management and the Office of the Inspector General (OIG) noted progress in establishing a more robust program. Several initiatives are planned in FY 2017. Specifically, NARA has acquired the full range of services from FireEye that will provide Host and Network based protection, along with 24/7 monitoring and Email Threat Prevention. NARA is also continuing its partnership with DHS on the Continuous Diagnostics and Mitigation (CDM) program, Risk Vulnerability Assessment and HVA Security Architecture Review. Further, NARA has funded its efforts to complete Unprivileged and Privileged user Personal Identity Verification (PIV) card implementation. These actions will further strengthen the agency's ability to effectively protect its assets and improve its FISMA and Cybersecurity CAP Goal performance.

## Inspector General Assessment

**Identify** Level 1: Ad-Hoc  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 2: Defined

The OIG evaluation reviewed 11 NARA systems, and found that NARA made significant efforts to address weaknesses identified in previous FISMA evaluations and audit engagements. Examples of some of these efforts include, and are not limited to the following:

- Designation of Information System Security Officers (ISSOs) to perform security support services.
- Identification of individuals with elevated security responsibilities for Tier-II security and privacy awareness training and the Logical Access Control System.
- Development and deployment of Tier-II security and privacy awareness training and the insider threat program.

As a result, we determined NARA's overall security and privacy training program was effective for this evaluation period. However, NARA still needs significant improvement in seven of the eight metric domains to be consistent with FISMA. All of the 20 recommendations from the previous year's FISMA audit remained unaddressed at the time of the FY 2016 evaluation. With the designation of the ISSOs, we expect further improvement to NARA's information security program will be realized in the next reporting period and years to come.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Metric	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	0%
Software Asset Management	0%	0%	0%
Vulnerability Management	70%	100%	100%
Secure Configuration Management	✓ 99%	100%	100%
Unprivileged User PIV Implementation	15%	0%	0%
Privileged User PIV Implementation	✓ 86%	86%	0%
Anti-Phishing Defenses	4	6	6
Malware Defenses	✓ 1	3	3
Other Defenses	✓ 2	3	3

### US-CERT Incidents by Attack vector

Total Number of Incidents: 30

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	1
Other	28
Multiple Attack vectors	0





# Cybersecurity Performance Summary

National Capital Planning Commission

## Chief Information Officer Assessment

The National Capital Planning Commission (NCPC) adopted the NIST Framework for Improving Critical Infrastructure Cybersecurity. Based on a self-assessment of the five functional areas, NCPC shows progress and is on target to strengthen its cybersecurity posture and close most identified gaps.

In FY 2016, NCPC made the most progress in the Identify and Protect functions. NCPC identified mission essential systems, and it assessed and authorized two systems. To protect the network, NCPC enforced multi-factor authentication using Personal Identity Verification (PIV) cards for logical access to the NCPC network. The self-assessment also determined that NCPC continues to make progress in meeting Cybersecurity CAP Goal targets. Of the nine FY 2016 CAP Goal capability area targets, NCPC met or exceeded five.

NCPC is participating in the DHS Continuous Diagnostics and Mitigation (CDM) Program. NCPC expects to implement a shared service solution in FY 2017 for hardware asset management, software asset management, configuration management, and vulnerability management.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for NCPC was not performed for FY 2016 and this section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of the Inspector General (OIG) appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. NCPC will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	90%	90%	100%
Vulnerability Management	80%	80%	0%
Secure Configuration Management	92%	92%	96%
Unprivileged User PIV Implementation	0%	0%	89%
Privileged User PIV Implementation	0%	75%	0%
Anti-Phishing Defenses	4	4	5
Malware Defenses	✓ 3	3	3
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Credit Union Administration

## Chief Information Officer Assessment

The National Credit Union Administration's (NCUA) information security program policies, technology, and practices are continuously maturing to align with the dynamic nature of the cybersecurity threats facing the nation and NCUA. Over the past year, NCUA has made significant progress in meeting the requirements of the OMB and NIST. Additionally, NCUA continues to proactively conduct ongoing assessments of the continued effectiveness of its program and implement an array of solutions toward achieving and maintaining its target maturity level(s).

Specific to the CAP Goals, our holistic solutions to address the Hardware Asset, Software Asset and Vulnerability Management CAP Goals has been acquired, piloted, and is either implemented or in an implementation phase currently but not in place by the October audit period. We continue to work through our Information Sharing Agreement requirements with State Examiners to further address our remaining Unprivileged User PIV Implementation metrics.

Hardware Asset Management scores from FY 2015 to FY 2016 dropped due to a change in the scoring methodology. Last year our approach for identifying and quarantining unauthorized assets did not require the additional component of notification. We have since added the notification components.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 1: Ad-hoc
- Recover** Level 3: Consistently Implemented

The NCUA Office of Inspector General (OIG) determined that NCUA's Office of the Chief Information Officer (OCIO) conducted an extensive review of NCUA's information security program this year. In addressing and resolving prior year FISMA issues and recommendations, NCUA has continued to strengthen its information security program during FY 2016.

OCIO's effort along with the FISMA audit resulted in the OIG reporting seven information security program areas in which NCUA needs to make improvements. Specifically, those areas are configuration management, incident response, contingency planning, account management, oversight of contractor systems, and plan of action and milestones; and with its system security plan. The OIG made 23 recommendations, which would help NCUA continue to improve the effectiveness of its information security program.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	0%
Software Asset Management	0%	0%	0%
Vulnerability Management	10%	22%	
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	74%	
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 6	6	6
Malware Defenses	✓ 4	4	4
Other Defenses	✓ 2	2	2

### US-CERT Incidents by Attack vector

Total Number of Incidents: 4

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	1
Loss or Theft of Equipment	1
Web	0
Other	1
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Endowment for the Arts

## Chief Information Officer Assessment

National Endowment for the Arts (NEA) is taking a hybrid approach following the guidelines established by the DHS Continuous Diagnostics and Mitigation (CDM) program. NEA is working under this guidance to enhance NEA's ability to identify and respond to the risk of emerging cyber threats. This hybrid approach allows NEA to tailor its information security practices to the agency's own mission, operation, and needs.

In FY 2016, NEA met eight of nine of the CAP Goal capability area targets. Of particular note, NEA implemented software to track hardware on its network, allowing it to meet the Hardware Asset Management CAP Goal capability area target. NEA will continue to improve to ensure efficiency, effectiveness and accountability of cybersecurity to the NEA and the Federal Government.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 3: Consistently Implemented
<b>Respond</b>	Level 4: Managed and Measureable
<b>Recover</b>	Level 1: Ad-Hoc

NEA operates at a maturity level of Consistently Implemented and overall security controls are automated where possible, operating as intended, and monitored effectively. NEA's success in addressing information security requirements is due primarily to its early adoption of the "shared services model" to obtain Managed Trusted Internet Protocol Services that is compliant with OMB security guidance. In addition, NEA has joined DHS's EINSTEIN Program, which supports Federal agencies in their efforts to comply with Congressional requirements for information security, including compliance with information assurance guidelines prepared by OMB. While security controls are operating as intended and being monitored, NEA is working to improve organization-wide risk management, maintenance of Plan of Actions and Milestones, enforcement of Personal Identity Verification (PIV) cards in multifactor authentication, and the level of instructional detail in contingency and disaster plans.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 99%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 2	2	3
Other Defenses	✓ 2	2	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 2

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	1
Other	0
Multiple Attack vectors	0

## Chief Information Officer Assessment

The National Endowment for the Humanities (NEH) made significant progress in its cybersecurity program and information technology (IT) infrastructure in the past year. Hardware and software assets are configured by following NIST guidelines. NEH uses multiple real-time monitoring systems, web filtering, and participates in the National Cybersecurity Assessment and Technical Services cyber hygiene program. NEH has a single connection to the internet through a Managed Trusted Internet Protocol Services Trusted Internet Connection, and it is in the process of becoming a participant in the EINSTEIN 3 Accelerated (E<sup>3</sup>A) program. Traffic through the agency's TIC is scanned for nefarious activity by the agency's Internet Service Provider. No high-severity attacks were successful against the agency during the past year. NEH improved their Distributed Denial of Service (DDOS) attack protection by purchasing a DDOS attack mitigation service from its TIC provider. NEH implemented multi-factor authentication where appropriate, such as on its virtual private network connection, and implemented the United States Government Computer Baseline configuration on its desktop workstations. NEH requires all employees to receive annual security awareness training; our compliance rate was 100% this year. Personnel with system administration and security responsibilities received additional security-specific training.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 2: Defined
<b>Respond</b>	Level 3: Consistently Implemented
<b>Recover</b>	Level 2: Defined

Over the years, NEH has realized steady progress in the implementation of an information security program consistent with FISMA and NIST requirements. However, the size of the agency and budgetary constraints have presented challenges in NEH's ability to fully implement core elements of information security continuous monitoring (ISCM) and contingency planning, which limits the overall effectiveness of the NEH information security program. The NEH risk management policy defines an organization-wide risk management strategy consistent with NIST requirements. However, the ISCM component of the strategy has not been fully implemented. The Agency's risk management policy prescribes the periodic conduct of information system-level risk assessments that integrate risk decisions from organizational and mission/business process perspectives. Such risk assessments have not been updated for the Agency's three moderate impact-level systems. The NEH must update system-level risk assessments and create continuous monitoring plans for the three systems. Furthermore, NEH's implementation of a comprehensive continuity of operations program (COOP) is not consistent. COOP testing/training has not been performed since fiscal year 2012.

## CAP Goal Metrics

✓ CAP Goal Met      ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	91%	0%
Software Asset Management	0%	0%
Vulnerability Management	54%	88%
Secure Configuration Management	99%	88%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	2	5
Malware Defenses	1	1
Other Defenses	0	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 6

Attack Vector	Number of Incidents
Attrition	1
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	4
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Labor Relations Board

## Chief Information Officer Assessment

National Labor Relations Board (NLRB) experienced no major incidents as defined in the OMB Memorandum M-16-03 during FY 2016. Additionally, the Agency had no events that would have necessitated a report to the DHS United States Computer Emergency Readiness Team (US-CERT).

Since the last report, NLRB continued its progress for certain administration priorities and key FISMA metrics. This progress included active participation in the Continuous Diagnostics and Mitigation (CDM) program and improving hardware/software asset management, network access control, configuration settings management and vulnerability and malware management. Additionally, NLRB continues to leverage DHS Shared Services, including subscribing to threat intelligence feeds through EINSTEIN 3 Accelerated (E<sup>3</sup>A) and the use of Trusted Internet Connections/E<sup>3</sup>A analytics.

During the next fiscal year, NLRB intends to fully implement the CDM program. In addition, the NLRB is committed to improving its performance in other areas, particularly with requiring the use of Personal Identity Verification (PIV) cards for authentication by March 31, 2017.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 2: Defined  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 1: Ad-Hoc  
**Recover** Level 3: Consistently Implemented

The Office of Inspector General (OIG) found that NLRB Office of the Chief Information Officer (OCIO) could improve the information technology (IT) security internal control environment by developing more thorough documentation of its policies and procedures and recording activities. As detailed in the FISMA responses, NLRB OCIO continues to rely heavily on an ad hoc approach. Additionally, OIG observed that some IT security processes, such as providing security training to new employees, are ignored. Two areas that could use significant improvement are the mandatory use of two-factor authentication to access NLRB's network and full implementation of the CDM program. Both areas are to be completed during FY 2017. The new Chief Information Officer has shown a significant interest in improving NLRB's IT security environment. Overall, there has been some improvement in NLRB's IT security function since the prior FISMA report.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	✓ 99%	■	■
Vulnerability Management	✓ 99%	■	■
Secure Configuration Management	✓ 96%	■	■
Unprivileged User PIV Implementation	6%		■
Privileged User PIV Implementation	63%	■	■
Anti-Phishing Defenses	4	■	■
Malware Defenses	4	■	■
Other Defenses	3	■	■

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Mediation Board

## Chief Information Officer Assessment

The National Mediation Board (NMB) system security program was significantly enhanced during FY 2016. These improvements included the completion of existing Plan Of Action and Milestones and a third party audit of the agency's system. NMB increased compliance with the Software Asset Management CAP Goal capability area target, primarily due to an increase in the Inventory Capability and Detect Block Unauthorized Software metric. NMB began analyzing 100% of all incoming email traffic, using sender authentication protocols and sender reputation filters.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for NMB was not performed for FY 2016 and this section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an Office of the Inspector General (OIG) appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. NMB will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	0%		
Vulnerability Management	0%		
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	3	5	5
Malware Defenses	2	4	4
Other Defenses	0	1	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Science Foundation

## Chief Information Officer Assessment

The National Science Foundation (NSF) is a small, single-mission agency. NSF has a strong, comprehensive, risk-based information technology (IT) security and privacy program. NSF works diligently to comply with Federal mandates and to implement tools to protect agency information and information resources.

NSF has a lean and proactive security team working continuously to improve its security posture. NSF takes a risk-based approach and prioritizes security risks and initiatives. NSF welcomes shared services to augment its capabilities, e.g. Trusted Internet Connections and Continuous Diagnostics and Mitigation (CDM). NSF is committed to a secure environment. Its dedicated staff continues to advance its IT security initiatives.

In FY 2016, NSF increased the percentage of the organization's unclassified networks assessed for vulnerabilities using Security Content Automation Protocol validated products.

NSF completed the DHS CDM Program Phase One to fortify its cybersecurity posture. NSF is enhancing its malware defense by enhancing current email and web traffic filtering. Privileged user access is being strengthened through PIV authentication. NSF's move to a new headquarters building in 2017 will include a new segmented network with multiple firewalls.

## Inspector General Assessment

<b>Identify</b>	Level 3: Consistently Implemented
<b>Protect</b>	Level 3: Consistently Implemented
<b>Detect</b>	Level 4: Managed and Measureable
<b>Respond</b>	Level 4: Managed and Measureable
<b>Recover</b>	Level 5: Optimized

In order to assess how NSF established its agency-wide information security program and practices, as required by FISMA, independent auditors performed detailed testing of NSF's general support system, and two major applications for compliance with selected NIST Special Publication 800-53 Revision 4 controls. Overall, the information security program was rated positively, but the auditors determined that continued management attention is necessary as NSF has not yet implemented all the requirements of the OMB guidance and NIST Special Publications in 6 of 57 security metrics found in the six non-maturity model domains. For both Information Security Continuous Monitoring and Incident Response and Reporting, NSF achieved a maturity rating of Level 3 Consistently Implemented for Processes and Technology and Level 4 Managed and Measurable for People.

NSF should continue to strengthen its security vulnerability resolution process and control over privileged accounts. In addition, NSF should continue to strengthen its contingency planning, interconnection security agreements, and accreditation package processes.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	0%	1%	1%
Vulnerability Management	88%	95%	95%
Secure Configuration Management	✓ 98%	100%	100%
Unprivileged User PIV Implementation	✓ 87%	93%	93%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	5	5
Malware Defenses	1	1	1
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 27

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	6
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	1
Other	20
Multiple Attack vectors	0



# Cybersecurity Performance Summary

National Transportation Safety Board

## Chief Information Officer Assessment

The National Transportation Safety Board's (NTSB) information technology (IT) security program established its overall framework by implementing and adopting guidance from the NIST Computer Security Division and the OMB Circular A-130 directives. This body of policies and operating bulletins serve as the primary source of IT security guidance for NTSB management, IT security professionals, and users throughout the organization. These policies also apply to all Federal employees and contract support staff employed by or working for NTSB. In addition, these policies apply to all NTSB IT systems, including hardware, software, media, facilities, and data owned or in the custody of NTSB. They also apply to any outside organizations, or their representatives, who are granted access to NTSB IT resources, including other Federal departments and agencies.

NTSB met four out of nine CAP Goal capability areas in FY 2016, including Hardware Asset Management, Vulnerability Management, Secure Configuration Management, and Malware Defense. The Vulnerability Management CAP Goal capability area was met due to an increase in the percent of the organization's unclassified networks assessed for vulnerabilities using Security Content Automation Protocol-validated products. NTSB did not meet the Software Asset Management target, specifically due to a decrease in the Detect Block Unauthorized Software metric.

## Inspector General Assessment

- Identify** Level 5: Optimized
- Protect** Level 3: Consistently Implemented
- Detect** Level 5: Optimized
- Respond** Level 5: Optimized
- Recover** Level 3: Consistently Implemented

An independent auditor prepared the audit report. The scope of the review covered IT security program policies and procedures issued by the Agency. It tested a sample of the NTSB's systems to determine whether the Agency had implemented required management, operational, and technical controls. Additionally, auditors held meetings with NTSB officials, observed IT security operations, and performed various tests on IT controls implemented by the agency. Lastly, they reviewed the continuous monitoring program established by the Agency. The Office of Inspector General (OIG) concluded that NTSB developed and implemented an IT security program that met FISMA requirements. However, the audit identified that there were certain aspects of its IT security program that could be strengthened, including actions related to PIV usage, compliance with OMB Circular A-123, and developing goals, action plans, and timelines associated with alternate site controls for management and governance personnel.

### CAP Goal Metrics

✓ CAP Goal Met      ■ 2015 ■ 2016

Category	2015 (%)	2016 (%)
Hardware Asset Management ✓	90%	95%
Software Asset Management	75%	0%
Vulnerability Management ✓	75%	100%
Secure Configuration Management ✓	55%	99%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	3
Malware Defenses ✓	0	3
Other Defenses	0	1

### US-CERT Incidents by Attack vector

Total Number of Incidents: 2

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	2
Multiple Attack vectors	0





# Cybersecurity Performance Summary

Nuclear Regulatory Commission

## Chief Information Officer Assessment

The Nuclear Regulatory Commission (NRC) continues its efforts towards full compliance with FISMA targets and with the agency's Privacy Management Program. The current number of reportable systems at NRC stands at 22. During FY 2016, the agency completed security assessments and approved change authorizations for each system. NRC has had no major security incidents since last year's report, and it continues to make progress towards meeting the CAP Goal targets. In the upcoming year, NRC expects to make progress towards updating its authorization program, implementing additional personal identity verification, reducing the risk of malware, and addressing audit findings.

NRC improved its Anti-Phishing Defense, with all incoming email traffic now being analyzed, using sender authentication protocols and reputation filters.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 1: Ad-Hoc
- Recover** Level 3: Consistently Implemented

Policies and procedures have been developed for the eight areas in the Office of Inspector General (OIG) CyberScope metrics. All 22 of NRC's operational information systems have been authorized to operate. However, NRC information technology (IT) security program policies and procedures are not consistently implemented. The FY 2016 independent evaluation identified three repeat findings: Continuous monitoring is not performed as required; NRC system inventory is not up-to-date; and the agency did not provide sufficient documentation to determine if oversight of contractor systems is adequate.

Timely remediation of weaknesses identified during periodic system cybersecurity assessments continues to be a challenge. The configuration, vulnerability, and patch management processes continue to be concerns for the majority of NRC's systems. Finally, some metrics were found to be "Not Met" because NRC did not provide requested documentation.

To improve NRC's implementation of FISMA, the OIG made five recommendations. Management stated their general agreement with the findings and recommendations in this report. OIG will check the agency's progress in implementing the recommendations in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	92%	92%	90%
Vulnerability Management	✓ 96%	96%	100%
Secure Configuration Management	✓ 99%	99%	99%
Unprivileged User PIV Implementation	✓ 93%	93%	99%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	4	4	7
Malware Defenses	2	2	3
Other Defenses	✓ 2	2	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 25

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	1
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	7
Loss or Theft of Equipment	2
Web	0
Other	14
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Nuclear Waste Technical Review Board

## Chief Information Officer Assessment

The Nuclear Waste Technical Review Board (NWTRB) is an independent Small Agency. NWTRB's leadership is committed to efficiently utilizing resources to ensure the agency's information systems are secure. Despite limited personnel resources, NWTRB continues to make progress towards meeting the goals of the President's Management Council and developing a fully matured information security program. NWTRB has not yet met or exceeded all CAP Goals at this time, despite addressing seven of nine goals. Of the nine CAP Goals for FY 2016, NWTRB currently exceeds targets for six of the goals, is addressing one of the goals through the utilization of non-technical means, and anticipates meeting targets of the final two goals by Quarter 2 of FY 2017.

## Independent Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 2: Defined
- Recover** Level 5: Optimized

An independent evaluation of the status of the FISMA program for NWTRB was not performed for FY 2016 and this section is marked "Not Applicable". Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. NWTRB will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	0%		
Software Asset Management	0%		
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%		
Privileged User PIV Implementation	0%		
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 4	4	4
Other Defenses	✓ 2	2	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Occupational Safety and Health Review Commission

## Chief Information Officer Assessment

The Occupational Safety and Health Review Commission (OSHRC) remains abreast of additions and changes to the FISMA. The Commission's security program continues to be incorporated into its annual performance and security plans, providing reasonable assurance and safeguards to maintain integrity and competence. Furthermore, OSHRC practices delegation of authority as a structured organization with defined separation of duties and supervision.

Two-factor Personal Identity Verification (PIV) card or NIST Level of Assurance 4 credential compliance increased, meeting the CAP Goal target for Unprivileged User PIV Implementation.

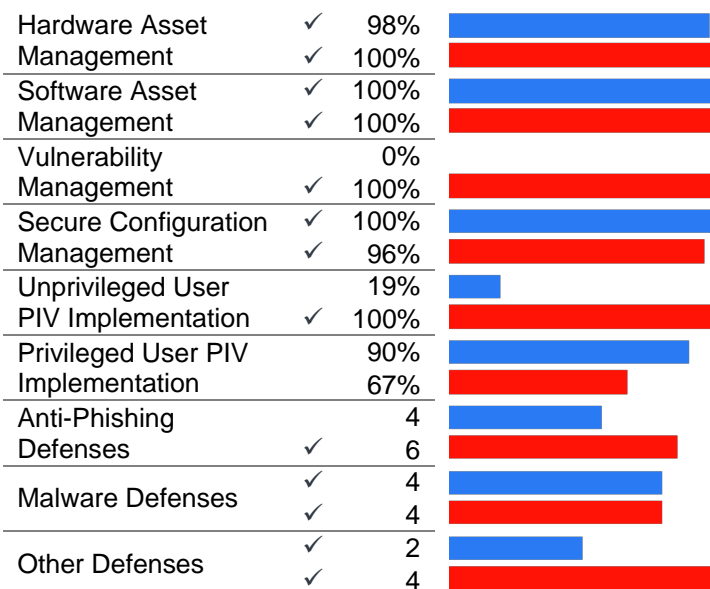
## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for OSHRC was not performed for FY 2016 and this 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. OSHRC will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Office of Government Ethics

## Chief Information Officer Assessment

The Office of Government Ethics (OGE) remains committed to maintaining an information technology (IT) security program that takes a risk-based approach to protect the confidentiality, integrity, and availability of OGE systems and data. No major incidents occurred during this reporting period. OGE IT security program highlights are as follows: OGE was one of the first agencies to fully implement the Managed Trusted Internet Protocol Service, which plays an active role in protecting the agency's network; it was also one of the first agencies to fully implement Internet Protocol version 6 (IPv6) in accordance with OMB mandates; OGE's private network is scanned for vulnerabilities on a weekly basis by the National Cybersecurity Assessment and Technical Services team at the DHS; OGE is participating as a charter member of the Continuous Diagnostics and Mitigation (CDM) Program managed by DHS, and actively participates in meetings, conference calls, and the ongoing procurement process; OGE has fully deployed Personal Identity Verification (PIV) card authentication on the agency's network; and OGE's IT specialists continuously monitor the security of the agency's information technology resources. Two-factor authentication is required to access the OGE network locally and remotely. Additionally, OGE conducts annual cybersecurity awareness classes. OGE notes that the variance in percentages for asset management between FY 2015 and FY 2016 is due to a change how OGE measured hardware assets; OGE measured laptops in FY 2016, but not in FY 2015.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for OGE was performed for FY 2015. An independent assessment was not performed in FY 2016, so this section is marked "Not Applicable" (NA).

OGE performed a self-assessment in FY 2016 using the same network vulnerability tool used by the independent evaluator. OGE collaborated with the independent assessor to configure the tool using the same configuration used by the independent evaluator. OGE runs the tool on a monthly basis. As a result, OGE's internal network is scanned for known vulnerabilities on a monthly basis instead of annually, allowing OGE to be more proactive in the mitigation of vulnerabilities found. 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 will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	54%
Software Asset Management	✓ 100%	100%	44%
Vulnerability Management	0%	0%	0%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	NA	7	7
Malware Defenses	NA	4	4
Other Defenses	NA	4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Office of Navajo and Hopi Indian Relocation

## Chief Information Officer Assessment

The Office of Navajo and Hopi Indian Relocation (ONHIR) is switching to a new Managed Trusted Internet Protocol Services service provider that will enable the agency to take advantage of the DHS's EINSTEIN 3 Accelerated (E<sup>3</sup>A) program and services.

As ONHIR improves the security of its system, it will work with the DHS Continuous Diagnostic and Mitigation (CDM) Program to address ONHIR's gaps, identify specific recommendations, and subsequently create new priorities.

ONHIR is behind on Personal Identity Verification (PIV) card implementation due to issuance problems. This will be corrected by the Interior Business Center within the next four to six months and will then be deployed for use on the agency network. Of additional note, ONHIR is estimated to close down on September 30, 2018.

Additionally, the percentage of privileged users technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance 4 credential increased from FY 2015 to FY 2016, surpassing the CAP Goal for Privileged User PIV Implementation.

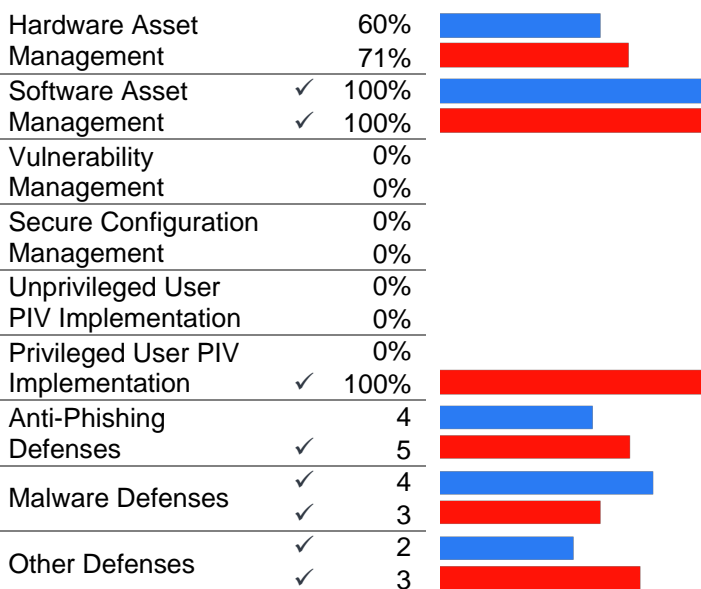
## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for ONHIR was not performed for FY 2016 and this 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. ONHIR will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Office of Personnel Management

## Chief Information Officer Assessment

In FY 2016, Office of Personnel Management (OPM) consolidated cybersecurity functions under a newly-created Chief Information Security Officer (CISO). Over 20 new employees have been hired to join the cybersecurity program, including additional Information System Security Officers to support all OPM major information systems. With the support provided by the consolidation under the CISO, an authorization to operate (ATO) sprint initiative was started in order to obtain a current ATO for all OPM major information systems and resolve the outstanding material weakness in the program. By the end of FY 2016, OPM obtained 18 ATOs with several others in progress. OPM plans to have current ATOs for all systems by the end of the calendar year.

OPM security operations implemented capabilities to strengthen the security of the overall environment in support of a new defense-in-depth architecture including enrolling in the Einstein 3 Accelerated (E<sup>3</sup>A) program to further increase visibility and to detect and block potential incidents. Also, OPM became the first agency to implement phase one capabilities of the Continuous Diagnostics and Mitigation (CDM) program. OPM continues to work towards the second phase of the CDM program to support trust in people granted access, security-related behavior, credentials and authentication, and privilege management.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 2: Defined

This audit rolls forward a material weakness related to OPM's Security Assessment and Authorization (Authorization) program. At the end of FY 2016, OPM still had at least 18 major systems without a valid authorization in place. However, OPM has recently placed significant effort toward meeting authorization requirements. This audit re-opens a significant deficiency related to OPM's information security management structure. Although OPM has developed a structure that the Office of the Inspector General (OIG) believes can be effective, there has been a high turnover rate of critical positions. The negative impact of these issues is apparent in the results of our current FISMA audit work. There has been a significant regression in OPM's compliance with FISMA requirements. OPM has placed effort toward filling these positions, but simply having the staff on board does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA requirements. OIG will continue to closely monitor activity in this area throughout FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 95%	95%	100%
Secure Configuration Management	✓ 100%	100%	98%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	5	7
Malware Defenses	✓ 4	4	5
Other Defenses	✓ 3	3	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 169

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	13
External/Removable Media	2
Impersonation/Spoofing	1
Improper Usage	9
Loss or Theft of Equipment	20
Web	5
Other	116
Multiple Attack vectors	3



# Cybersecurity Performance Summary

Office of Special Counsel

## Chief Information Officer Assessment

Office of Special Counsel (OSC) made significant strides in modernizing its information technology (IT) architecture and bolstering its cybersecurity workforce in FY 2016. Specifically, OSC leveraged the FedRAMP services to modernize general support systems and improved IT governance by identifying key IT performance metrics and developed its first-ever Enterprise Risk Management Council to track its plan of action and milestones. OSC improved its capabilities to support an agile, secure and modern work environment. OSC will implement several key security capabilities provided by DHS-led Continuous Diagnostic & Mitigation (CDM) in FY 2017 as a Small Agency early CDM adopter and forefront of the Task Order 2 Group F Deployment.

Overall, OSC demonstrated concrete year-over-year improvement from its FY 2015 FISMA baseline. Its CAP Goal performance excelled in three out of nine capabilities. This improvement is attributed to improved performance related to Secure Configuration Management, Anti-Phishing Defense, and Other Defenses.

## Inspector General Assessment

<b>Identify</b>	Level 2: Defined
<b>Protect</b>	Level 2: Defined
<b>Detect</b>	Level 1: Ad-Hoc
<b>Respond</b>	Level 2: Defined
<b>Recover</b>	Level 5: Optimized

An independent consulting firm conducted an audit of OSC's FISMA metrics. The audit followed the scope and format of the FY 2016 Annual FISMA Inspector General (IG) Report. The auditor issued recommendations about each aspect of the NIST Cybersecurity Framework. The audit recognized that OSC has a developing IT security program and needs additional resources to continue improving network and system protection, detection and automation objectives. Furthermore, it recommended that OSC implement Identity, Credential, and Access Management tools and strengthen its Risk Management processes. Other recommendations included implementing multi-factor authentication, performing formal system risk assessments, and improving internal controls governance.

In summary, OSC completed key IT infrastructure modernization objectives and implemented essential security best practices. The agency introduced new IT processes and adopted Continuity of Operations and Incident Response Plan to strengthen its organizational resiliency. OSC has a developing information security continuous monitoring strategy and faces challenges in its risk management program due to lack of adequate resources and funding.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	0%	0%
Vulnerability Management	0%	0%
Secure Configuration Management	0%	97%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	6
Malware Defenses	1	0
Other Defenses	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	1
Other	0
Multiple Attack vectors	0

### Chief Information Officer Assessment

The Overseas Private Investment Corporation’s (OPIC) information security program is divided into six areas. OPIC has assessed each area as follows:

- **Policy:** Strong. While some procedures might need to be updated, as a whole, OPIC has ample documentation on the why and how of its security program and practice.
- **Training:** Strong. 100% of privileged users and 92% of staff have completed trainings within OPIC parameters.
- **Security Engineering:** Strong. OPIC has implemented boundary protection technologies, an Intrusion Detection System (solution, anti-malware, and process monitoring tools). It also collects indicators of compromise, and is able to analyze multiple data points to detect malicious activities.
- **Risk Monitoring:** Good. OPIC scans continuously for vulnerabilities and configuration deviations. However, OPIC does not have automatic capabilities to block new assets or unauthorized software.
- **Incident Response:** Fair. While OPIC has a strong incident response team, it has to update its current incident response plan with the latest response, containment, and remediation techniques. OPIC also needs to conduct training exercises and test the IR plan.
- **Compliance:** Good. A repeatable process is in place to ensure that OPIC can meet reporting and security requirements mandated by law.

### Inspector General Assessment

- Identify** Level 3: Consistently Implemented
- Protect** Level 2: Defined
- Detect** Level 3: Consistently Implemented
- Respond** Level 2: Defined
- Recover** Level 5: Optimized

The Office of Inspector General contracted with an independent certified public accounting firm to conduct an audit to determine whether OPIC implemented certain security controls for selected information systems in support of FISMA. The firm tested OPIC’s implementation of selected controls outlined in NIST Special Publication 800-53, Revision 4. The audit reviewed four OPIC systems.

Overall, OPIC implemented 84 of 105 selected security controls for the four selected information systems in support of FISMA. Although OPIC had policies for its information security program, its implementation of those policies was not always fully effective. Specifically, OPIC did not implement 21 controls designed to preserve the confidentiality, integrity, and availability of the Agency’s information and information systems. The audit made 17 recommendations to strengthen OPIC’s information security program, including configuration management, account management, asset management, and physical and environmental controls. Detailed audit findings and recommendations to address identified weaknesses are outlined in Audit Report No. A-OPC-17-005-C, which can be found on the OIG’s website.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	5%	6%
Vulnerability Management	60%	100%
Secure Configuration Management	100%	96%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	5
Malware Defenses	2	3
Other Defenses	1	4

### US-CERT Incidents by Attack vector

Total Number of Incidents: 9

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	7
Web	1
Other	1
Multiple Attack vectors	0





# Cybersecurity Performance Summary

Peace Corps

## Chief Information Officer Assessment

The Peace Corps' Office of the Chief Information Officer (OCIO) has made significant steps towards improving its cybersecurity program. In FY 2014, an audit found that the Peace Corps had not fully captured FISMA reportable systems within its Cybersecurity Assessment and Management tool and did not have adequate contingency plans or incident response plans. Since that time, coverage of network monitoring capabilities has been increased to cover basic foundational goals. FISMA-reportable systems are incorporated into the CSAM tool for ongoing assessment and authorization, tracking, and closing Plan of Action and Milestones records. The Peace Corps has also developed an updated incident response plan and contingency plans for FISMA reportable systems.

The Peace Corps demonstrated improvement in CAP Goal performance in FY 2016, meeting four out of nine capabilities. This improvement is attributed to improved performance related to unauthorized hardware assets, visibility capability, and security configuration management metrics.

## Inspector General Assessment

**Identify** Level 1: Ad-Hoc  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 2: Defined  
**Recover** Level 1: Ad-Hoc

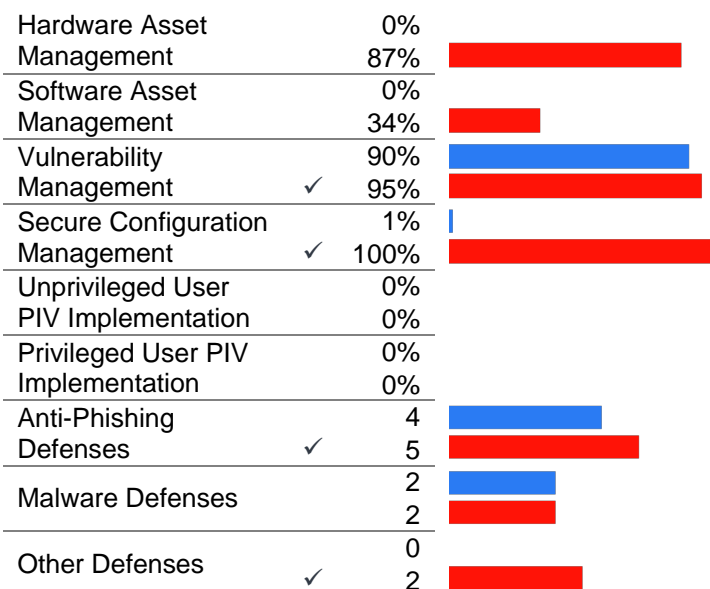
Peace Corps lacks an effective information security program because of problems related to people, processes, technology, and culture. Furthermore, the Office of Inspector General (OIG) found weaknesses across all of the FISMA-reportable areas. There are several FISMA findings that have been outstanding for over seven years and the agency has struggled to implement corrective actions.

OIG is concerned about the quality of the information technology (IT) security program, especially considering the sensitive data that the Peace Corps maintains. Without a comprehensive, integrated IT security program, sensitive agency systems and data are vulnerable to exploitation and failure.

Peace Corps will need to place a sharper focus on improving its IT security program by assigning sufficient qualified personnel, and prioritizing the time and resources necessary to become fully FISMA compliant and eliminate weaknesses. Implementation of the Risk Management Framework will facilitate the tailoring of an information security program that meets Peace Corps' mission and business needs across a decentralized organization.

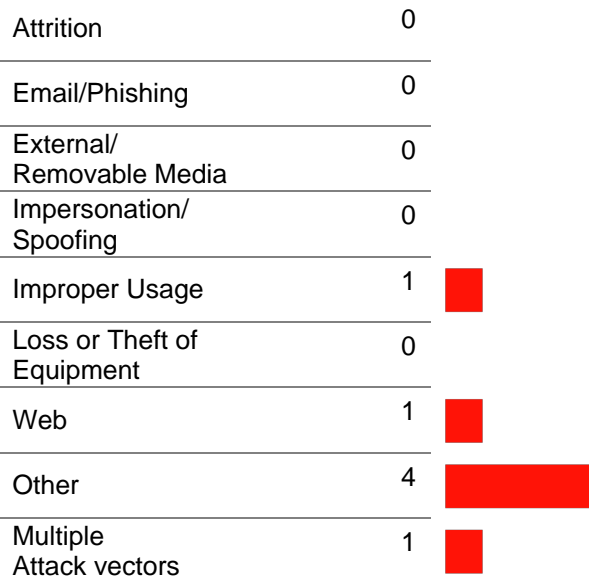
## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016



## US-CERT Incidents by Attack vector

Total Number of Incidents: 7





# Cybersecurity Performance Summary

Pension Benefit Guaranty Corporation

## Chief Information Officer Assessment

Pension Benefit Guaranty Corporation (PBGC) has continued to make numerous improvements to its security and privacy programs, including addressing previous FISMA challenges by updating its enterprise cybersecurity policies to align with current internal and external requirements. The policies will foster NIST Special Publication 800-53 Revision 4 transition by authorizing a risk management framework to require ongoing authorizations via continuous monitoring and leverage the implementation of updated security controls with identified parameters. PBGC will also supplement these policies by revising its independent risk management framework and security authorization requirements for information systems. Subsequent trainings and communication will be coordinated to raise awareness on the updated efforts. The agency continues to mature its security program areas and focus additional efforts on implementing the Administration's priority cybersecurity capabilities. While the agency has met some of the FY 2016 cybersecurity CAP Goal targets, it recognizes the need to continue making progress in three areas: Information Security Continuous Monitoring, Identity, Credential, and Access Management, and Anti-Phishing & Malware Defense. They have been identified in PBGC's Information Technology (IT) Strategic Plan as performance measures are projected for significant increases. PBGC will closely monitor its progress toward making timely corrections to all noted deficiencies.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

PBGC made progress in addressing weaknesses in its entity-wide security program. In FY 2016, the Agency made progress in implementing its risk management function by publishing its Information Security Risk Management Framework process, however, work still remains. PBGC has an acting risk executive but needs to permanently fill the position and document organizational risk tolerance. PBGC has implemented a tool as the Agency's official repository for security controls but needs to remain diligent to ensure that NIST Special Publication 800-53 Revision 4 controls are fully and consistently implemented. Similarly in the area of ICAM, PBGC made progress enforcing the use of Personal Identity Verification (PIV) cards for authentication for privileged and non-privileged users but still needs to focus on ensuring accounts are recertified timely and unnecessary accounts are removed. PBGC's ISCM policies, procedures, and strategies are still in the implementation phase and the ISCM program is in the process of maturing and not consistently implemented. Review of system level ISCM plans identified that 3 of 18 plans had not been completed and finalized.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 99%	99%	99%
Software Asset Management	91%	94%	94%
Vulnerability Management	2%	99%	99%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	9%	97%	97%
Privileged User PIV Implementation	63%	100%	100%
Anti-Phishing Defenses	4	4	4
Malware Defenses	1	3	3
Other Defenses	1	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 51

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	3
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	2
Loss or Theft of Equipment	27
Web	15
Other	4
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Postal Regulatory Commission

## Chief Information Officer Assessment

The Postal Regulatory Commission (Commission) is pleased to report that during FY 2016, the agency did not have any cybersecurity or personally identifiable information (PII) incidents. During this fiscal year, the Commission strengthened its overall information security program by diligently working to identify and detect cybersecurity incidents and to protect its systems, assets, data, and capabilities from cybersecurity risks. The Commission improved its overall security posture by implementing new realtime scanning and monitoring capabilities to proactively identify and detect threats to our IT systems. This ensures the continued delivery of information technology (IT) services that support the Commission's mission without any disruption.

The Commission also worked to ensure that its continuity, response, and recovery plans are resilient and ready to use. The Commission tests and refines its Continuity of Operations and Disaster Recovery capabilities annually to ensure essential mission functions can be performed during any emergency or other situations that disrupt normal operations.

With new security threats continually emerging, the Commission developed projects to comply with FISMA guidance and other cybersecurity initiatives (e.g., Managed Trusted Internet Protocol Services, EINSTEIN 3 Accelerated (E<sup>3</sup>A), and Continuous Diagnostics and Mitigation (CDM)); updated its security practices and policies to protect sensitive information; and educated employees about existing and emerging cyber threats.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for the Commission was not performed for FY 2016 and this section is marked "Not Applicable" (NA). The Commission's Office of Inspector General plans to submit the results of an independent evaluation of the Commission's FISMA program for FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met      ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 95%	95%	0%
Software Asset Management	✓ 95%	95%	0%
Vulnerability Management	✓ 95%	95%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	5	4
Malware Defenses	✓ 3	3	5
Other Defenses	1	1	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Privacy and Civil Liberties Oversight Board

## Chief Information Officer Assessment

Privacy and Civil Liberties Oversight Board (PCLOB) has made significant progress to strengthen its infrastructure cybersecurity controls over this reporting cycle. PCLOB has enhanced its capabilities to detect hardware and software changes with automated tools. PCLOB has implemented 100% use of Personal Identity Verification (PIV) cards across its network. As a small agency, PCLOB has leveraged DHS resources to implement security base practices and initiatives. PCLOB plans to be an early Continuous Diagnostics and Mitigation (CDM) adopter for their group level to supplement existing mitigation tools. PCLOB has identified the need for additional staff, new tools and improvements to current change management.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for PCLOB was not performed for FY 2016 and this 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. PCLOB will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	79%	79%	100%
Vulnerability Management	0%	0%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	5	6
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 1	1	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Railroad Retirement Board

## Chief Information Officer Assessment

The Railroad Retirement Board (RRB) continues to progress towards a compliant information security program to improve the RRB's security posture. RRB has implemented an Information Security Continuous Monitoring Strategy, as outlined in the OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, which aggressively addresses gaps in its information security program. RRB has also enrolled in the DHS Continuous Diagnostics and Mitigation (CDM) Program to improve its ISCM strategy pertaining to vulnerability assessment, hardware and software asset management, configuration management, and privileged account management. RRB has also enrolled in the DHS EINSTEIN 3 Accelerated (E<sup>3</sup>A) program, which ensures that all of the Domain Name System and Simple Mail Transfer Protocol are monitored.

RRB increased its CAP Goal target from three in FY 2015 to four of the nine capabilities in FY 2016. RRB did not meet the CAP goal target for Hardware Asset Management in FY 2016 as it did in FY 2015. However, RRB met the target for Secure Configuration Management and Other Defenses, and improved in Vulnerability Management and Malware Defense. RRB also demonstrated improvement in its implementation for Personal Identity Verification (PIV) card usage for unprivileged and privileged users although these did not meet the CAP Goal target.

## Inspector General Assessment

**Identify** Level 3: Consistently Implemented  
**Protect** Level 1: Ad-Hoc  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 2: Defined  
**Recover** Level 2: Defined

RRB continues to make progress towards the implementation of an information security program that is consistent with the FISMA, but it has not yet established an effective program. During FY 2016, RRB improved its contingency planning program by completing action to transition the backup of exchange and open systems to their offsite disaster recovery facility. However, the Office of Inspector General (OIG) assessment of RRB's overall information security program maturity results in a rating of 'Not Effective' for each of the eight domains evaluated. Deficiencies were identified in the areas of risk management, contractor systems, configuration management, identity and access management, security and privacy training, continuous monitoring management, incident response and reporting, and contingency planning.

Recommendations for improvement to RRB management are related to assorted policies, procedures, and time standards; exploring new automated technology products; access control; training; updating agency records; and implementing stronger controls.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	50%
Software Asset Management	0%	0%	0%
Vulnerability Management	93%	100%	100%
Secure Configuration Management	✓ 99%	100%	100%
Unprivileged User PIV Implementation	50%	50%	78%
Privileged User PIV Implementation	0%	51%	51%
Anti-Phishing Defenses	3	3	3
Malware Defenses	2	3	3
Other Defenses	✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 69

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	15
External/Removable Media	1
Impersonation/Spoofing	1
Improper Usage	18
Loss or Theft of Equipment	27
Web	0
Other	6
Multiple Attack vectors	1



# Cybersecurity Performance Summary

Securities and Exchange Commission

## Chief Information Officer Assessment

The Securities and Exchange Commission (SEC) continued to enhance its operational security capabilities through the continued development of an Information Security Continuous Monitoring (ISCM) program and the continued investment and implementation of proactive security capabilities and detection mechanisms and numerous application and database security and vulnerability assessment tools. In support of the ISCM program, SEC deployed an integrated information security compliance management capability to serve as a centralized repository for the management of SEC's FISMA compliance obligations, information system Plans of Action and Milestones, and incident tracking and response efforts. The SEC also made significant progress towards previously identified opportunities to improve agency compliance with Personal Identify Verification (PIV) controls. The SEC is committed to protecting information originating from within the Agency and data provided to SEC from registrants and other parties by adhering to a framework that focuses on implementing management, operational and technical security controls when implementing technologies or information systems. In FY 2017, the SEC will remain focused on efforts to continuously strengthen the agency's cybersecurity posture and protect information stored, processed, and transmitted by agency information systems.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 3: Consistently Implemented
- Recover** Level 3: Consistently Implemented

The SEC information security program does not meet the FY 2016 Inspector General (IG) FISMA Reporting Metrics' definition of "Effective." The information security program is considered ineffective because its overall maturity did not reach Level 4, Managed and Measurable. The FY 2016 IG FISMA Reporting Metrics states "all things being equal, Level 4, Managed and Measurable, represents an effective information security program."

During the SEC IG's assessment of the eight FISMA metric domains, opportunities were identified for improvement and recommendations will be made to the Agency in a report to be issued in early 2017.

### CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	0%
Software Asset Management	✓ 100%	100%	0%
Vulnerability Management	65%	65%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	0%	0%	34%
Privileged User PIV Implementation	40%	40%	0%
Anti-Phishing Defenses	3	5	5
Malware Defenses	2	3	3
Other Defenses	2	2	4

### US-CERT Incidents by Attack vector

Total Number of Incidents: 43

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	15
External/Removable Media	1
Impersonation/Spoofing	0
Improper Usage	2
Loss or Theft of Equipment	0
Web	11
Other	14
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Selective Service System

## Chief Information Officer Assessment

The Selective Service System (SSS) is in overall compliance with the FISMA requirements for FY17. SSS developed an agency-wide program to provide security for information and information systems to support the operations and assets of the Agency. The audit team assessed compliance with OMB Circular A-130 and concluded that SSS was in full compliance with FISMA requirements with no material weaknesses.

The objective of the audit was to assess whether SSS had developed, documented, and implemented an Agency-wide information security program in accordance with OMB Circular A-130, FISMA, and NIST Special Publication 800-53, and other metrics to include: Agency IT security policy and procedures; performance tests on general support systems and major applications; observed IT security observations; and continuous diagnostics and mitigation programs established by the SSS.

SSS met the CAP goal for all nine capabilities in FY 2016, with performance improvements shown in metrics related to vulnerability and weakness management, Anti-Phishing Defense, Malware Defense, and other related defenses.

The auditors determined that SSS had developed an agency-wide IT security program based upon assessed risk, and that the security program provided reasonable assurance that the Agency's information and information systems are appropriately protected. There were no findings or recommendations requiring a written response from the SSS.

## Independent Assessment

<b>Identify</b>	Level 5: Optimized
<b>Protect</b>	Level 5: Optimized
<b>Detect</b>	Level 5: Optimized
<b>Respond</b>	Level 5: Optimized
<b>Recover</b>	Level 3: Consistently Implemented

The independent assessor assessed whether SSS had developed, documented, and implemented an agency-wide information security program, as required by the OMB Circular A-130 and FISMA. To accomplish this objective, a sample of controls contained in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, were reviewed for IT security program policies and procedures issued by the agency; tested on the agency's general support system and its major application to determine whether the agency had implemented required management, operational, and technical controls; and reviewed for the Continuous Diagnostics and Mitigation (CDM) program established by the agency.

The independent assessor concluded that SSS was in overall compliance with FISMA requirements and determined that SSS had developed an agency-wide IT security program based upon assessed risk, and the security program provided reasonable assurance that the agency's information and information systems are appropriately protected.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Metric	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 95%	95%	100%
Secure Configuration Management	✓ 100%	100%	98%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 6	6	7
Malware Defenses	✓ 4	4	5
Other Defenses	✓ 4	4	4

## US-CERT Incidents by Attack vector

Total Number of Incidents: 21

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	21
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Small Business Administration

## Chief Information Officer Assessment

The Small Business Administration (SBA) information security program continues to improve. SBA has made significant strides in implementing repeatable, reportable, and recordable processes across all information security continuous monitoring (ISCM) areas. The main highlights include: migration of all systems from NIST Special Publication 800-53 Revision 3 to Revision 4; implementing an approved Incident Response Plan; instituting a biannual Incident Response Plan training program; and deploying a fully operational 24x7 Security Operations Center, which has enabled SBA to meet the United States Computer Emergency Readiness Team (US-CERT) one-hour incident response reporting requirement and exceed its malware and blended defense targets, respectively. SBA has begun to implement its approved ISCM plan and mature its continuous monitoring and assessment process, to include Cloud Services, within the constraints of available resources.

## Inspector General Assessment

- Identify** Level 2: Defined
- Protect** Level 2: Defined
- Detect** Level 2: Defined
- Respond** Level 2: Defined
- Recover** Level 5: Optimized

The FISMA requires the Inspectors General to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices. The scope of this evaluation was to test and assess the effectiveness of information security policies, procedures, and practices.

The SBA Office of Inspector General (OIG) evaluation determined that SBA progressed from a primarily Level 1, Ad-Hoc maturity level to primarily Level 2, Defined. In addition, significant improvement was observed in the Recover area, where the evaluation results yielded a Level 5, Optimized designation, which exceeded the threshold required to be deemed "Effective."

OIG determined that the SBA had achieved Level 2, Defined in FY 2016 for the areas of Identify, Protect, Detect, and Respond. However, based on maturity level ranking criteria, OIG determined that the agency's programs in these areas were "Not Effective."

The OIG initiated improvement recommendations in areas where new vulnerabilities were identified and continues to monitor outstanding recommendations.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 98%	98%	98%
Software Asset Management	2% 9%	2%	9%
Vulnerability Management	✓ 99% ✓ 100%	99%	100%
Secure Configuration Management	✓ 98% 2%	98%	2%
Unprivileged User PIV Implementation	✓ 89% ✓ 99%	89%	99%
Privileged User PIV Implementation	✓ 100% ✓ 100%	100%	100%
Anti-Phishing Defenses	4 4	4	4
Malware Defenses	1 ✓ 4	1	4
Other Defenses	✓ 2 ✓ 2	2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 223

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	52
External/Removable Media	0
Impersonation/Spoofing	1
Improper Usage	5
Loss or Theft of Equipment	19
Web	83
Other	58
Multiple Attack vectors	5





# Cybersecurity Performance Summary

Smithsonian Institution

## Chief Information Officer Assessment

The Smithsonian Institution (SI) has very complex and conflicting security needs. SI must balance its researchers' needs for collaboration and information sharing, its museums' needs to become more interactive and technology-driven, and its commercial and fundraising elements' Payment Card Industry requirements, Federal mandates, and protection of personally identifiable information (PII). SI also has many closely integrated partners that operate at least partially on the agency's network, along with a diverse user base that includes many volunteers, visiting research fellows, emeritus scholars, and other affiliated personnel, for which there is constant turnover.

SI has many critical security program elements in place, including perimeter protections, malware defense, vulnerability management, training/awareness, incident response, and Assessment and Authorization. Significant improvements have been made in these areas; however, there is still much work to be done. SI has a plan and is implementing enhancements as quickly as possible with the resources available. In order to ensure that risk is adequately managed to address all diverging needs, SI is developing an enterprise security architecture that takes into account its diverse business needs, compliance requirements, risk factors, and best practices. This will be used to ensure that the roadmap for security improvements is based on requirements and a clear prioritized strategy.

## Inspector General Assessment

- Identify** Level 1: Ad-Hoc
- Protect** Level 1: Ad-Hoc
- Detect** Level 1: Ad-Hoc
- Respond** Level 1: Ad-Hoc
- Recover** Level 1: Ad-Hoc

The SI Office of the Inspector General contracted with an independent auditor to perform an audit of SI's information security program and practices. Although not subject to FISMA, the Smithsonian has adopted FISMA through its policy because it is consistent with and advances the Smithsonian's mission and strategic goals.

The independent auditor determined that in FY 2016, SI did not have an effective organization-wide information security program. For example, SI had not implemented an Information Security Continuous Monitoring strategy and had not identified and implemented a centralized technology solution to effectively monitor data and information system risks. Furthermore, SI had not consistently implemented a security assessment and authorization process.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	0%	0%
Software Asset Management	49%	49%
Vulnerability Management	29%	99%
Secure Configuration Management	0%	7%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	3	5
Malware Defenses	0	2
Other Defenses	2	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 36

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	7
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	2
Loss or Theft of Equipment	8
Web	7
Other	8
Multiple Attack vectors	4



# Cybersecurity Performance Summary

Social Security Administration

## Chief Information Officer Assessment

Social Security Administration (SSA) practices a Defense-in-Depth cyber strategy that employs strong security controls, policies and technologies to manage risk in accordance with the NIST Cybersecurity Framework. In FY 2016, SSA made substantial progress in all areas of the framework. SSA developed the first enterprise cybersecurity strategy and met all government-wide performance goals. SSA extended the risk management process for its centralized and contractor systems to include its regional systems. SSA issued its first provisional cloud authorization to operate (ATO) by leveraging FedRAMP. SSA strengthened its access controls with its automated Security Access Management portal and Security Administration Reports Application, and established an authoritative contractor database. SSA piloted its automated Access Removal Tool and acquired a new solution to strengthen its privileged account management. SSA strengthened its vulnerability management by implementing new technology and improving its alert process. Nearly 85,000 of its users completed their annual security training and conducted exercises to test their ability to detect social engineering attacks. SSA has a comprehensive incident response process with the capability to report personally identifiable information (PII) losses and security operation center incidents to United States Computer Emergency Readiness Team (US-CERT). SSA established continuity plans and conducted business impact analysis to determine potential adverse impact on its operations.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 2: Defined  
**Detect** Level 3: Consistently Implemented  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 3: Consistently Implemented

An independent public accountant firm was contracted to perform the FISMA review. Although SSA had established an information security program and practices across the agency, the results identified a number of control deficiencies related to Configuration Management, Contingency Planning, Contractor Systems, Identity and Access Management, Incident Response, Information Security Continuous Monitoring, Risk Management, and Security and Privacy Training. The weaknesses identified may limit the SSA's ability to protect adequately the organization's information and information systems.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 100%	100%	100%
Software Asset Management	✓ 100%	100%	100%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 86%	86%	99%
Privileged User PIV Implementation	✓ 99%	99%	100%
Anti-Phishing Defenses	✓ 6	6	5
Malware Defenses	✓ 3	3	4
Other Defenses	✓ 3	3	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 1,626

Attack Vector	Number of Incidents
Attrition	69
Email/Phishing	26
External/Removable Media	1
Impersonation/Spoofing	3
Improper Usage	196
Loss or Theft of Equipment	43
Web	40
Other	1,221
Multiple Attack vectors	27



# Cybersecurity Performance Summary

Surface Transportation Board

## Chief Information Officer Assessment

The Surface Transportation Board (STB) has continued to make progress establishing its own information security program since becoming an independent agency in December 2015. In FY 2016, STB met seven out nine CAP Goal capabilities, including Vulnerability Management, Secure Configuration Management, Unprivileged User Personal Identity Verification (PIV) card Implementation, Privileged User PIV card Implementation, Anti-Phishing Defenses, Malware Defenses, and Other Defenses. While STB has made significant progress in reaching its FISMA metrics and CAP Goal targets, the Board has identified gaps, specifically in with regard to automated hardware notifications, that it is actively working to address. To accomplish this, STB is working with DHS to implement the Continuous Diagnostics and Mitigation (CDM) program and other tools acquired on its behalf.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for STB was not performed for FY 2016 and this 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. STB will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	NA	0%
Software Asset Management	NA	61%
Vulnerability Management	✓ 100%	100%
Secure Configuration Management	✓ 98%	98%
Unprivileged User PIV Implementation	✓ 97%	97%
Privileged User PIV Implementation	✓ 100%	100%
Anti-Phishing Defenses	✓ 5	5
Malware Defenses	✓ 3	3
Other Defenses	✓ 2	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Tennessee Valley Authority

## Chief Information Officer Assessment

The mission of Tennessee Valley Authority's (TVA) information security program is to strengthen the reliability, availability, and resilience of electronic and information-based assets by ensuring that leadership, processes, measures, and operational capabilities align to TVA's mission.

TVA believes its cybersecurity program is operating more effectively than indicated by this year's new FISMA maturity measurement methodology. Other utility-specific audits and external evaluations of TVA's cybersecurity program have indicated the program is highly effective as did last year's FISMA evaluation.

TVA is fully focused and engaged on the further expansion and development of its current cybersecurity capabilities, with a specific focus on integrating information and operational technology, establishing a proactive security posture, and focusing on security with compliance as a by-product. Three of TVA's primary goals are:

- Monitoring and Incident Response : expansion of capabilities in TVA's operational environment;
- Controls Consolidation: development of a unified controls framework, and;
- Organizational Improvements: people, processes, and facilities.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 1: Ad-Hoc  
**Respond** Level 2: Defined  
**Recover** Level 3: Consistently Implemented

The FY 2016 FISMA independent evaluation by TVA OIG of the TVA's information security program found multiple deficiencies in practices and component parts of the program. During the past two fiscal years, TVA had made improvements in the domains of Protect and Recover. Conversely in FY 2016, TVA's Identify and Respond domains were found to be not effective based on incomplete system categorizations and authorizations and due to an incomplete incident response skills assessment and integration with Information Security Continuous Monitoring (ISCM). In addition, TVA had taken actions to strengthen its information security program by planning implementation of an agency-wide ISCM program, however it is currently at an Ad Hoc level.

The OIG recommended that TVA's Chief Information Officer perform a risk assessment of the FY 2016 FISMA metrics not met and determine actions necessary to reduce cybersecurity risk to the agency in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	10%	59%
Software Asset Management	1%	1%
Vulnerability Management	64%	50%
Secure Configuration Management	✓ 100%	80%
Unprivileged User PIV Implementation	0%	0%
Privileged User PIV Implementation	0%	0%
Anti-Phishing Defenses	4	4
Malware Defenses	1	2
Other Defenses	✓ 3	✓ 3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 51

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	7
External/Removable Media	3
Impersonation/Spoofing	0
Improper Usage	22
Loss or Theft of Equipment	11
Web	3
Other	5
Multiple Attack vectors	0



# Cybersecurity Performance Summary

United States Access Board

## Chief Information Officer Assessment

The United States Access Board (USAB) is taking steps to continually improve information security. In the last year, USAB has implemented security information and event management for continuously collecting, monitoring, and alerting security events to the system. Additionally, USAB has a log collection and retention program, which is used to investigate support remediation for any security incidents. The agency also has endpoint security compliance of its servers, including all patch delivery to endpoints, and it engages in monitoring and management of its enterprise infrastructure for hardware and software vulnerabilities. USAB implemented a managed help desk solution for its agency network and security issues, and is aware that its information security practices must be improved in the areas of asset and configuration management, boundary protection, training, and education.

USAB has started developing an authorization to operate (ATO) process of its system. USAB anticipates that the completion of the ATO in FY 2017 will provide an enhanced security baseline, a completed system security categorization, contingency and incident response plan, security awareness training plan, and a system security plan. USAB believes that the implementation of managed security services and active participation in Continuous Diagnostics and Mitigation (CDM) Program meetings and CDM Learning will help the agency accomplish its goal of improving its information security baseline.

## Independent Assessment

<b>Identify</b>	NA
<b>Protect</b>	NA
<b>Detect</b>	NA
<b>Respond</b>	NA
<b>Recover</b>	NA

An independent evaluation of the status of the FISMA program for USAB was not performed for FY 2016 and this 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. USAB will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	50%	50%	0%
Software Asset Management	0%	0%	0%
Vulnerability Management	✓ 100%	100%	100%
Secure Configuration Management	✓ 100%	100%	100%
Unprivileged User PIV Implementation	✓ 100%	100%	100%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	2	2	3
Malware Defenses	✓ 4	2	4
Other Defenses	✓ 3	1	3

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0



# Cybersecurity Performance Summary

United States Agency for International Development

## Chief Information Officer Assessment

The United States Agency for International Development's (USAID) information security program implements and monitors security controls to protect information systems in accordance with the risk and magnitude of harm that would result from unauthorized access, use, or disclosure. The USAID program serves 12,250 users and 81 missions. Program objectives include: testing policies/procedures/plans; assessments of controls; focused security training; remedial action; and incident detection, reporting, and response. Core functions include: establishing security policy; implementing security risk management; developing compliance standards; conducting independent compliance audits; coordinating system Accreditation and Authorization oversight; monitoring information system contracts; conducting reporting activities; enacting cyberspace initiatives; representing security interests at Chief Information Officer Governance boards; overseeing security training; performing e-Discovery activities; overseeing OMB-DHS integration/cross-government priorities; overseeing Section 508 compliance; responding to cybersecurity/privacy incidents; and implementing anti-malware tools/capabilities. Chief program activities: supporting the Cybersecurity National Action Plan; implementing Federal Information Technology Acquisition Reform Act (FITARA); and investing in additional cloud security applications.

## Inspector General Assessment

**Identify** Level 2: Defined  
**Protect** Level 3: Consistently Implemented  
**Detect** Level 2: Defined  
**Respond** Level 3: Consistently Implemented  
**Recover** Level 5: Optimized

The Office of Inspector General (OIG) contracted with an independent certified public accounting firm to conduct an audit to determine whether USAID implemented selected security controls for selected information systems in support of the FISMA. The firm tested USAID's implementation of selected controls outlined in NIST Special Publication 800-53, Revision 4. The audit reviewed five systems.

Overall, USAID implemented 126 of 144 selected security controls for the 5 selected information systems. Although USAID generally had policies and procedures for its information security program, its implementation of those policies for 18 of the 144 selected controls was not fully effective to preserve the confidentiality, integrity, and availability of USAID's information and information systems. The audit made 20 recommendations to strengthen USAID's information security program, including the organizational structure for the Office of the Chief Information Officer and controls over patch and configuration management and system authorizations. Detailed audit findings and recommendations to address identified weaknesses are outlined in Audit Report No. A-000-17-001-C, which can be found on the OIG's website.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015 ■ 2016

Category	✓ CAP Goal Met	2015	2016
Hardware Asset Management	✓ 95%	100%	95%
Software Asset Management	0%	100%	0%
Vulnerability Management	✓ 100%	100%	41%
Secure Configuration Management	75%	89%	75%
Unprivileged User PIV Implementation	28%	100%	28%
Privileged User PIV Implementation	✓ 100%	100%	100%
Anti-Phishing Defenses	✓ 5	6	5
Malware Defenses	2	3	2
Other Defenses	✓ 3	3	2

## US-CERT Incidents by Attack vector

Total Number of Incidents: 131

Attack Vector	Number of Incidents
Attrition	0
Email/Phishing	8
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	2
Loss or Theft of Equipment	8
Web	20
Other	93
Multiple Attack vectors	0



# Cybersecurity Performance Summary

Vietnam Education Foundation

## Chief Information Officer Assessment

As a small agency of four employees, which will sunset in calendar year 2018, Vietnam Education Foundation (VEF) lacks the resources to fully implement some of the CAP Goal performance requirements.

In FY 2016, VEF met one out of the nine capabilities. VEF met five out of seven capability areas for the Anti-Phishing Defenses CAP Goal which requires all incoming email traffic to pass through an anti-phishing and anti-spam filtration at the outermost border mail agent or server, and a having a reputation filter that performs a threat assessment of the sender. VEF did not report on the CAP Goal Metrics in FY 2015.

## Independent Assessment

**Identify** NA  
**Protect** NA  
**Detect** NA  
**Respond** NA  
**Recover** NA

An independent evaluation of the status of the FISMA program for VEF was not performed for FY 2016 and this 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. VEF will explore contracting with an independent assessor in FY 2017.

## CAP Goal Metrics

✓ CAP Goal Met    ■ 2015    ■ 2016

Category	2015	2016
Hardware Asset Management	NA	0%
Software Asset Management	NA	0%
Vulnerability Management	NA	0%
Secure Configuration Management	NA	0%
Unprivileged User PIV Implementation	NA	0%
Privileged User PIV Implementation	NA	0%
Anti-Phishing Defenses	NA	5 ✓
Malware Defenses	NA	1
Other Defenses	NA	1

## US-CERT Incidents by Attack vector

Total Number of Incidents: 0

Attrition	0
Email/Phishing	0
External/Removable Media	0
Impersonation/Spoofing	0
Improper Usage	0
Loss or Theft of Equipment	0
Web	0
Other	0
Multiple Attack vectors	0

## Section II: FY 2016 Agency Performance

### C. FY 2016 Major Information Security Incidents<sup>13</sup>

Agency heads determined that sixteen of the 30,899 incidents reported in FY 2016 met the threshold of a major incident, a designation that triggers mandatory steps for agencies including reporting certain information to Congress. OMB defined the term major incident, in [OMB Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements](#). In determining whether a “major incident” has occurred, agencies shall consider whether the incident:

1. Involves information that is Classified, Controlled Unclassified Information (CUI) proprietary, CUI Privacy, or CUI Other; ;
2. Is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and,
3. Has a high or medium functional impact to the mission of an agency; or
4. Involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:
  - a. 10,000 or more records or 10,000 or more users affected; or,
  - b. Any record that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in a significant or demonstrable impact on agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

OMB refined the definition of major incident in [OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements](#). Specifically, the new guidance redefined major incident as any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. OMB M-17-05 also directed agencies to [NIST Special Publication 800-61, Computer Security Incident Handling Guidance](#), and the DHS [National Cybersecurity and Communications Integration Center Cybersecurity Incident Scoring System](#), which uses the following factors for determining the impact of an incident: functional impact, observed activity, location of observed activity, actor characterization, information impact, recoverability, cross-sector dependency, and potential impact.

OMB M-17-05 also provided guidance on when a data breach constitutes a major incident. A breach constitutes a “major incident” when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals’ PII constitutes a major incident.



## Section II: FY 2016 Agency Performance

The following cyber events in FY 2016 were reported by agencies as meeting the threshold of major incident according to the definition in OMB M-16-03:

- **Department of Commerce** – In December 2015, the United States Patent and Trademark Office (USPTO) headquarters experienced a major power outage, which resulted in damaged equipment that required the subsequent shutdown of many systems, including the USPTO's Patent and Trademark filing, search, and fee payment systems, and a system that USPTO's patent examiners use. There were no reports of exploits or data breaches during the outage, indicating there were no external or internal threats, and no Controlled Unclassified Information was compromised.
- **Department of Health and Human Services (HHS)** – HHS reported one major incident in FY 2016, which involved the potential compromise of Personally Identifiable Information (PII). HHS reported the incident was reported in the last week of FY 2016 and notes that the investigation and mitigation steps will largely take place in FY 2017.
- **Department of Housing and Urban Development (HUD)** – HUD reported two major incidents in FY 2016. The first was uncovered in August 2016, when a member of the public notified the agency that PII, including Social Security numbers, were accessible via an internet-based Google search. The second incident included two separate instances in September 2016 involving public-facing HUD websites displaying PII related to HUD-assisted public housing. HUD is working to provide affected individuals with credit monitoring solutions.
- **Department of the Treasury (Treasury)** – Treasury reported two major incidents in FY 2016. Treasury detected a prior incident in January 2016 at the Internal Revenue Service (IRS). Treasury determined that an attacker was attempting to fraudulently generate Electronic Filing Personal Identification Numbers (PINs) based on taxpayer information stolen from non-IRS sources. Treasury offered affected individuals an identity protection PIN to protect against fraudulent returns in 2017. Treasury also detected an incident in September 2016, when a retiring Office of the Comptroller of the Currency employee downloaded a large volume of files to two thumb drives; Treasury has indicated that there is no evidence that the individual disclosed information, as the agency had previously encrypted the data.
- **Federal Deposit Insurance Corporation (FDIC)** – FDIC reported 10 major incidents in FY 2016, which generally stemmed from employees taking PII or other sensitive information on removable media in an unauthorized fashion. In response to these incidents, the FDIC implemented a technical solution that would prevent users, with limited exceptions, from downloading data to removable media. In addition, FDIC is continuing to offer credit monitoring to affected individuals.

## Section III: Enhancing Privacy Programs

### A. Progress in Meeting Key Senior Agency Officials for Privacy Measures

Protecting individual privacy is important. The Federal Government increasingly uses IT to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personal information. Federal agencies must continue taking steps to analyze and address privacy risks at the earliest stages of the planning process, and must continue to manage information responsibly throughout the information life cycle.

Federal agencies must continue to work with their Senior Agency Officials for Privacy (SAOPs) to ensure compliance with privacy requirements in law, regulation, and policy. Agencies are responsible for ensuring that all of their privacy impact assessments (PIAs) and system of records notices (SORNs) are complete and up-to-date. Moreover, agencies must continue to develop and implement policies that outline rules of behavior, detail training requirements for personnel, and identify consequences and corrective actions to address non-compliance. Finally, agencies must continue implementing appropriate breach response procedures and update those procedures when necessary.

All 24 CFO Act agencies and 51 non-CFO Act agencies reported privacy performance measures to OMB for FY 2016. The FISMA SAOP metrics assess agencies' implementation of critical privacy controls across agencies' information technology systems. It is important to note that, it is not possible to compare the FY 2016 performance measures and the FY 2015 performance measures because of significant changes to the underlying methodology for the FISMA SAOP metrics for FY 2016. In addition, OMB expects to significantly modify the FISMA SAOP metrics for FY 2017 to account for several major privacy-related policies that were recently issued or reissued. These policies include [OMB Circular A-130, Managing Information as a Strategic Resource](#) (Jul. 2016), [OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act](#) (Dec. 2016), and [OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information](#) (Jan. 2017).

### B. Information Systems – Privacy Impact Assessments

The implementation target for the Federal Government is for 100 percent of applicable systems to be covered by PIAs. In FY 2016, 77% of applicable systems reported by CFO Act agencies and 85% of applicable systems reported by non-CFO Act agencies had up-to-date PIAs. The 77% figure reported by CFO Act agencies represents a decrease from the 83% compliance rate reported in FY 2015. In contrast, the 85% figure reported by non-CFO Act agencies is the same as the compliance rate from FY 2015.

## Section III: Enhancing Privacy Programs

### C. Information Systems – System of Records Notices

Similar to PIAs, the goal for the Federal Government is to cover 100% of applicable systems in which agencies maintain records subject to the Privacy Act with a published and up-to-date SORN. In FY 2016, 82% of CFO Act agencies' and 84% of non-CFO Act agencies' systems with Privacy Act records reported having a published, up-to-date SORN. Both figures represent a decrease from the numbers reported in FY 2015.

**Table 7: CFO Act Agencies' Progress in Meeting Key SAOP Measures**

Key Privacy Performance Measures – CFO Act Agencies	FY 2014	FY 2015	FY 2016
Number of systems containing information in identifiable form	4,406	4,601	4,356
Number of systems requiring a PIA	2,701	2,940	3,128
Number of systems with a PIA	2,564	2,428	2,409
Percentage of systems with a PIA	95%	83%	77%
Number of systems requiring a SORN	3,346	3,414	3,515
Number of systems with a SORN	3,217	3,260	2,866
Percentage of systems with a SORN	96%	96%	82%

**Source:** Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2015, to September 30, 2016.

**Table 8: Non-CFO Act Agencies' Progress in Meeting Key SAOP Measures**

Key Privacy Performance Measures – Non-CFO Act Agencies	FY 2014	FY 2015	FY 2016
Number of systems containing information in identifiable form	758	745	621
Number of systems requiring a PIA	529	540	665
Number of systems with a PIA	436	457	563
Percentage of systems with a PIA	82%	85%	85%
Number of systems requiring a SORN	605	582	853
Number of systems with a SORN	553	525	717
Percentage of systems with a SORN	91%	90%	84%

**Source:** Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2015, to September 30, 2016.

### D. Privacy Training and Accountability

In FY 2016, all 24 CFO Act agencies reported that they developed and implemented policies to ensure that all employees and contractors with access to information resources receive privacy training, and that they have established rules of behavior for employees and contractors that have access to information resources. In addition, 22

## Section III: Enhancing Privacy Programs

out of the 24 CFO Act agencies reported that they require role-based privacy training for employees and contractors, and 21 CFO Act agencies reported that they developed and implemented a policy to ensure that employees and contractors are held accountable for complying with privacy requirements and managing privacy risks.

Moreover, in FY 2016, 46 out of 51 non-CFO Act agencies reported that they developed and implemented a policy to ensure that all employees and contractors with access to information resources receive privacy training, and 45 non-CFO Act agencies reported that they have established rules of behavior for employees and contractors that have access to information resources. In addition, 43 non-CFO Act agencies reported that they developed and implemented a policy to ensure that employees and contractors are held accountable for complying with privacy requirements and managing privacy risks. However, only 28 non-CFO Act agencies reported that they require role-based privacy training for employees and contractors.

**Table 9: Privacy Training and Accountability**

Privacy Training and Accountability	CFO Act Agencies	Non-CFO Act Agencies
Has the agency developed and implemented a policy to ensure that all employees and contractors with access to information resources receive privacy training?	100%	90%
Does the agency require role-based privacy training for employees and contractors who have particular responsibilities before authorizing access to information resources?	92%	55%
Has the agency established rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to information resources?	100%	88%
Has the agency developed and implemented a policy to ensure that employees and contractors are held accountable for complying with privacy requirements and managing privacy risks?	88%	84%

**Source:** Data reported to DHS via CyberScope and provided to OIRA from October 1, 2015, to September 30, 2016.

## Section IV: Appendices

### Appendix 1: IT Security Spending Reported by CFO Act Agencies

As the urgency of securing Federal systems and information continues to increase, the government will continue to commit considerable resources to strengthen Federal cybersecurity, including modernizing or replacing antiquated technology, streamlining disparate IT budgeting and governance structures, and reducing cybersecurity workforce shortages and skill gaps. OMB requires agencies to report cybersecurity-spending data to determine agency-specific cybersecurity needs and to understand how much agencies are spending in pursuit of a more secure Federal enterprise.

In FY 2016, OMB updated the way it captures information security spending by agencies. Utilizing the existing Capital Planning and Investment Control budget collection process, OMB Cyber reoriented its budget categories to relate to existing FISMA metric categories. The goal is to better map cybersecurity spending to agency performance on specific capabilities, to determine where gaps exist, and where agencies may need additional funding.

Table 10 reflects the total amount the civilian CFO Act agencies reported spending on relevant security investments in FY 2016.

**Table 10: FY 2016 Civilian CFO Agency IT Security Spending**

Agency	FY 2016 Spending (\$ in Millions)	Agency	FY 2016 Spending (\$ in Millions)
Commerce	\$101.03	NASA	\$143.74
DHS	\$1,283.99	NRC	\$20.14
DOT	\$86.55	NSF	\$10.79
ED	\$80.76	OPM	\$19.72
Energy	\$334.31	SBA	\$8.44
EPA	\$31.67	SSA	\$155.66
GSA	\$47.69	State	\$126.68
HHS	\$373.47	Treasury	\$396.20
HUD	\$3.00	USAID	\$25.13
Interior	\$73.49	USDA	\$67.99
Justice	\$206.54	VA	\$294.81
Labor	\$66.06	<b>Total</b>	<b>\$3,957.86</b>

## Section IV: Appendices

### Appendix 2: Acronyms and Abbreviations

Chief Financial Officer (CFO) – The official charged with overseeing all financial management activities relating to the programs and operations of an agency, per the Chief Financial Officer Act of 1990.

Chief Financial Officer (CFO) Act Agencies – CFO Act agencies are those agencies designated in the CFO Act (with the addition of DHS and minus the Federal Emergency Management Agency). In practice, the CFO Act agencies are the 24 largest Federal agencies in terms of budget; the 23 civilian CFO Act agencies are the CFO Act agencies minus the Department of Defense.

Chief Information Officer (CIO) – The official charged with executing the organization's information resource management activities as delegated by the organization's head, with duties set forth in 44 U.S.C. § 3506.

Chief Information Security Officer (CISO) – The official charged with developing, documenting, and implementing an agency's information security program.

Continuous Diagnostics and Mitigation (CDM) Program – a DHS-led program that provides commercial off-the-shelf tools and services that enable Federal, state, local, regional, and tribal governments to strengthen the security posture of their IT networks.

Council of Inspectors General on Integrity and Efficiency (CIGIE) – An independent entity established within the Executive Branch to address integrity, economy, and effectiveness issues that transcend individual government agencies and to aid in the establishment of a professional, well-trained and highly skilled workforce within the Offices of Inspectors General.

Cross-Agency Priority (CAP) Goals – Established by the Government Performance and Results Modernization Act of 2010, CAP Goals are a tool used to accelerate progress on a limited number of Presidential priority areas for which implementation requires active collaboration between multiple agencies, overcoming organizational barriers to achieve better performance than one agency can achieve on its own.

Cybersecurity National Action Plan – A national effort that tied near-term actions to a cohesive long-term strategy for the purpose of enhancing cybersecurity awareness and protections, safeguarding privacy, and maintaining public safety.

Federal Risk and Authorization Management Program (FedRAMP) – A GSA-led government-wide program that applies a standardized approach to validate commercial cloud products and services against Federal cybersecurity standards.

Fiscal Year (FY) – The Federal budgeting year, which extends from October 1st of each year to September 30th of the next year.

Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) – Issued by NIST in 2014, the Cybersecurity Framework is a risk-based set of industry standards and best practices to help organizations manage risks. In FY

## Section IV: Appendices

2016, both the CIO and IG FISMA metrics were aligned to the Cybersecurity Framework to provide a more thorough picture of agency cybersecurity activities.

Hardware Assets Management – The automated or manual management of agency endpoints, mobile devices, networking devices, and other input/output devices if they appear with their own address.

Highly Adaptive Cybersecurity Services (HACS) – IT security services added by GSA to Schedule 70 to provide agencies with quick, reliable access to key services before, during, and after cyber threats occur.

Identity, Credential, and Access Management (ICAM) – The implementation of a set of capabilities that ensure users must authenticate information technology resources and have access to only those resources that are required for their job functions.

Information Security Continuous Monitoring (ISCM) – The provision of ongoing observation, assessment, analysis, and diagnosis of an organization’s cybersecurity: posture, hygiene, and operational readiness.

Inspector General (IG) – An independent and objective unit established pursuant to the Inspector General Act of 1978 to conduct and supervise audits, inspections, and investigations of agency programs and operations.

Major Incident – OMB defined a major incident in [OMB Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements](#). In determining whether a “major incident” has occurred, agencies shall consider whether the incident:

1. Involves information that is Classified, Controlled Unclassified Information (CUI) proprietary, CUI Privacy, or CUI Other; ;
2. Is not recoverable, not recoverable within a specified amount of time, or is recoverable only with supplemental resources; and,
3. Has a high or medium functional impact to the mission of an agency; or
4. Involves the exfiltration, modification, deletion or unauthorized access or lack of availability to information or systems within certain parameters to include either:
  - a. 10,000 or more records or 10,000 or more users affected; or,
  - b. Any record that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in a significant or demonstrable impact on agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

OMB refined the definition of major incident in [OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements](#). Specifically, the policy redefined major incident as any incident that is likely to result in demonstrable harm to the national security interests, foreign relations,

## Section IV: Appendices

or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

National Cybersecurity Protection System and EINSTEIN – The goal of the National Cybersecurity Protection System, which includes EINSTEIN, is to provide the Federal Government with improved situational awareness of intrusion threats to Federal Executive Branch civilian networks and near real-time identification and prevention of malicious cyber activity.

Privileged User – A user with elevated privileges, typically a system administrator, network administrator, and others who are responsible for system/application control, monitoring, or administration functions.

Secure Configuration Management – The auditing of agency operating systems to ensure compliance with appropriate common security configuration baselines.

Software Asset Management – The capability to automatically inventory software assets and detect, alert, and/or block unauthorized software from executing.

United States Computer Emergency Readiness Team (US-CERT) – US-CERT is a division within DHS charged with responding to major information security incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

Unprivileged User – Any user that is not a privileged user.

Vulnerability Management – The capability to assess an organization's unclassified networks for security vulnerabilities, specifically using Security Content Automation Protocol (SCAP) validated products.



## Section IV: Appendices

---

<sup>1</sup> Agencies report on the implementation of CDM capabilities as part of the Information Security Continuous Monitoring metrics. OMB will continue to refine its performance metrics as the program continues to develop

<sup>2</sup> GSA Federal Acquisition Service Process Efficiency Study, March 31, 2013, as cited in the IT Schedule 70 Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers Interact Draft Solicitation Posting Fact Sheet, August 12, 2016.

<sup>3</sup> [OMB Memorandum M-16-03](#) describes CyberStat Reviews are evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing targeted, tactical actions to deliver desired results.

<sup>4</sup> The Government Performance and Results Act Pub. L. No 111-352, (Jan. 4, 2011) (codified at 31 USC § 1101, note).

<sup>5</sup> [FY 2016 FISMA CIO Metrics](#) define Hardware Asset Management as the automated and/or manual management of agency endpoints, mobile devices, networking devices, and other input/output devices if they appear with their own address.

<sup>6</sup> FY 2016 FISMA CIO Metrics defines Software Asset Management as the capability to automatically inventory software assets and detect, alert, and/or block unauthorized software from executing.

<sup>7</sup> FY 2016 FISMA CIO Metrics defines Vulnerability Management is the capability to assess an organization's unclassified networks for security vulnerabilities, specifically using Security Content Automation Protocol (SCAP) validated products.

<sup>8</sup> FY 2016 FISMA CIO Metrics defines Secure Configuration Management as the management and auditing of agency operating systems to ensure they are in compliance with appropriate common security configuration baselines.

<sup>9</sup> FY 2016 FISMA CIO Metrics defines a privileged user as a user with elevated privileges, typically a system administrator, network administrator, and others who are responsible for system/application control, monitoring, or administration functions. The metrics defines an unprivileged user as any user who is not a privileged user.

<sup>10</sup> 44 USC § 3553(c)(3) requires a summary of the independent evaluations; a summary of the IG/independent assessment can be found in each agency's one-pager.

<sup>11</sup> 44 USC § 3553(c)(1).

<sup>12</sup> [NIST Special Publication 800-61, Revision 2](#) lists common vectors that are the method attack and provides expansive definitions of the attack vectors cited in this report.

<sup>13</sup> 44 USC § 3553(c)(1)(2).



National Security Archive,  
Suite 701, Gelman Library, The George Washington University,  
2130 H Street, NW, Washington, D.C., 20037,  
Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)