ANNUAL REPORT TO CONGRESS:

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

OFFICE OF MANAGEMENT AND BUDGET

March 18, 2016

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

March 18, 2016

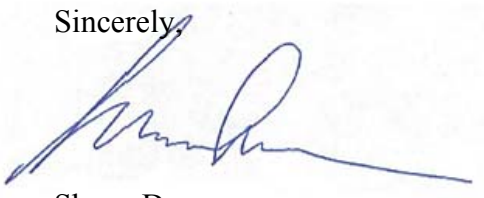
The Honorable Ronald Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

The attached report is submitted pursuant to Section 3553 of the Federal Information Security Modernization Act of 2014 (P.L. 113-283), which requires the Office of Management and Budget (OMB) to submit an annual report on the effectiveness of information security policies and practices during the preceding year and a summary of the evaluations conducted by agency Inspectors General. This report covers the period from October 1, 2014, through September 30, 2015, and provides an update of ongoing information security initiatives, a review of Fiscal Year 2015 information security incidents, Inspector General assessments of agencies' progress in implementing information security capabilities, and the Federal Government's progress in meeting key information security performance measures based on agency submitted data. As you will note, progress has been made in key areas of information security.

We appreciate the assistance of Congress in supporting these programs, and we look forward to continuing our work on this critical issue. Please contact the Office of Legislative Affairs at (202) 395-4790 if you have any questions.

Sincerely,



Shaun Donovan
Director

Enclosure

Identical Letter Sent to:

The Honorable Thomas R. Carper
The Honorable Jason Chaffetz
The Honorable Elijah Cummings
The Honorable Gene L. Dodaro
The Honorable Eddie Bernice Johnson
The Honorable Ron Johnson
The Honorable Michael McCaul
The Honorable Bill Nelson
The Honorable Lamar Smith
The Honorable Bennie G. Thompson
The Honorable John Thune

TABLE OF CONTENTS

EXECUTIVE SUMMARY

From the beginning of this Administration, the President has made it clear cybersecurity is one of the most important economic and national security challenges facing our Nation. For more than seven years, the Administration has acted comprehensively to confront this challenge and improve the Federal Government's cybersecurity. In February 2016, the Administration announced the *Cybersecurity National Action Plan (CNAP)*, which is the capstone effort that builds upon lessons learned from cybersecurity trends, threats, and intrusions. The CNAP directs the Federal Government to take a series of actions that will dramatically increase the level of cybersecurity in both the Federal Government and the Nation's digital ecosystem as a whole. The CNAP actions also build upon unprecedented progress to strengthen Federal cybersecurity that took place in Fiscal Year (FY) 2015 due to the efforts of the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and other Federal agencies. While this progress is encouraging, additional work remains to improve the defense of Federal systems, networks, and data from persistent threats and increasingly sophisticated malicious activity.

Throughout FY 2015, OMB, in coordination with the National Security Council (NSC) and DHS, executed a series of initiatives to improve Federal agencies' cybersecurity policies, procedures, and practices. OMB, in coordination with DHS, conducted evidence-based CyberStat Reviews to accelerate agency progress toward meeting government-wide performance goals and ensure that agencies are accountable for their cybersecurity posture. Additionally, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint, during which agencies immediately took steps to further protect Federal information and assets and improve the resilience of Federal networks. In particular, civilian agencies significantly improved their use of Strong Authentication Personal Identity Verification (PIV) cards, which can reduce the occurrence of certain types of cybersecurity incidents, from 42% to 72% during the Cybersecurity Sprint. As of November 16, 2015, Federal civilian agencies had further increased their use of PIV to 81%. – an increase of nearly 40% in less than a year. Following the Cybersecurity Sprint, OMB developed the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, which identifies a series of objectives and actions to further address critical cybersecurity priorities across the Federal Government.

To further this progress and support the CNAP, the FY 2017 President's Budget proposes investing over $19 billion in resources for cybersecurity. This includes creating the Information Technology Modernization Fund (ITMF), a revolving fund devoted to the retirement of the Government's antiquated information technology (IT) systems and transition to more secure and efficient modern IT systems, funding to streamline governance and secure Federal networks, and investments to strengthen the cybersecurity workforce and cybersecurity education across the Nation. While this funding is a necessary investment to secure our Nation in the future, we must continue to improve agencies' resilience to cybersecurity incidents in the near term. Despite unprecedented improvements in securing Federal information resources during FY 2015, malicious actors continue to gain unauthorized access to, and compromise, Federal networks, information systems, and data. During FY 2015, Federal agencies reported 77,183 cybersecurity incidents, a 10% increase over the 69,851 incidents reported in FY 2014. The increasing number and impact of these incidents demonstrate that continuously confronting cyber threats must remain a strategic priority.

Additionally, independent evaluations of information security programs and practices conducted by agency Inspectors General identified several performance areas in need of improvement, including configuration management, identity and access management, and risk management practices. Furthermore, Senior Agency Official for Privacy (SAOP) reviews found that Federal agencies must

continue to take steps to analyze and address privacy risks and ensure privacy protections are in place throughout systems' lifecycles.

In accordance with the *Federal Information Security Modernization Act of 2014* (FISMA), this report provides Congress information on agency progress towards meeting cybersecurity performance goals in FY 2015 and identifies 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. This report primarily includes FY 2015 data reported by agencies to OMB and DHS on or before November 16, 2015. Some sections also include data reported in previous fiscal years in order to provide trend information. Data that has become available since November 16, 2015, has also been included in some instances to provide up-to-date information. The report is organized as follows:

Section I: FY 2015 Federal Cybersecurity Overview
Describes the efforts undertaken during FY 2015 to protect existing and emerging Federal Government data and IT assets and the role OMB plays in Federal cybersecurity efforts.

Section II: Federal Cybersecurity Performance
Identifies agency performance against cybersecurity metrics and OMB's assessment of that performance.

Section III: Summary of Inspectors General Findings
Provides an overview of the assessments of agency Inspectors General (IG) regarding agency information security programs.

Section IV: Progress in Meeting Key Privacy Performance Measures
Provides an overview of the agency progress made in implementing steps to analyze and address privacy issues.

Section V: Appendices
Appendix 1: Security Incidents by CFO Act Agency
Appendix 2: Cybersecurity FY 2015 CAP Goal Metrics
Appendix 3: Information Security Spending Reported by CFO Act Agencies
Appendix 4: Inspectors General's Response
Appendix 5: List of CFO Act Agencies
Appendix 6: List of Non-CFO Act Agencies Reporting to CyberScope
Appendix 7: Acronyms

SECTION I: FY 2015 FEDERAL CYBERSECURITY OVERVIEW

Strengthening the cybersecurity of Federal networks, information systems, and data is one of the most important challenges facing the nation. To address this challenge, the Federal Government must take action to combat increasingly sophisticated and persistent threats posed by malicious actors. Accordingly, in FY 2015, OMB, DHS, and other Federal agencies executed a series of actions to secure information systems and bolster Federal cybersecurity. Although these actions led to areas of unprecedented improvement across the Federal Government, continued efforts are needed in order to preserve the progress that has been made and strengthen Federal cybersecurity well into the future. To this end, the CNAP is committing considerable resources to create the revolving ITMF to retire the Federal Government's antiquated IT systems and transition to more secure and efficient modern IT systems, funding to streamline governance and secure Federal networks, and investments to strengthen the cybersecurity workforce and cybersecurity education. This section highlights some of the FY 2015 initiatives aimed at strengthening Federal cybersecurity.

A. OMB'S ROLE IN FEDERAL CYBERSECURITY

In accordance with FISMA Section 3553, OMB is responsible for the oversight of Federal agencies' information security policies and practices. While agencies share the responsibility for Federal cybersecurity, the need for coordination across the Federal Government has grown in order to keep pace with increasing threats. Accordingly, OMB works to ensure that agencies are equipped with the proper tools and processes needed to enhance their cybersecurity capabilities. In FY 2015, OMB established the OMB Cyber and National Security Unit (OMB Cyber) within the Office of the Federal Chief Information Officer (OFCIO)[1] to expand its oversight of agency cybersecurity practices. OMB Cyber works to strengthen Federal cybersecurity through:

- Data-driven, risk-based oversight of agency and government-wide cybersecurity programs;
- Issuance and implementation of Federal policies to address emerging IT security risks; and,
- Oversight of the government-wide response to major incidents and vulnerabilities to reduce adverse impact on the Federal Government.

During FY 2015, OMB Cyber, in close coordination with NSC and DHS's National Protection and Programs Directorate, accelerated the adoption of Administration priorities through direct engagements with agency leadership and government-wide initiatives to address known cybersecurity gaps. The subsections below detail these activities and OMB Cyber's ongoing work to oversee and improve Federal agencies' cybersecurity performance.

B. CYBERSTAT REVIEWS

During FY 2015, OMB Cyber increased its oversight role and agency engagement through the CyberStat Review process.[2] CyberStat Reviews are comprehensive reviews of agency-specific cybersecurity posture. The purpose of the CyberStat Review is to accelerate progress toward achieving FISMA and Cross Agency Priority (CAP) goals by reviewing the progress of selected agencies, developing actionable plans, providing targeted assistance, and following up throughout the year.

OMB Cyber selected agencies for targeted oversight by analyzing incident data and risk factors related to key cybersecurity performance areas (e.g. Strong Authentication implementation). Leveraging increased resources provided by Congress in the *Consolidated and Further Continuing Appropriations*

Act, 2015 (P.L. 113-235), OMB Cyber set a goal of completing 12 Reviews in FY 2015 compared to four Reviews conducted in FY 2014. OMB Cyber exceeded its goal by completing 14 Reviews in FY 2015. Through these Reviews, OMB Cyber, DHS, and agency leadership collaborated to generate actionable recommendations to accelerate agency progress in implementing key cybersecurity priorities. Moreover, each Review served as an opportunity for OMB Cyber, DHS, and agency leadership to discuss agency successes and challenges, and share agency best practices to address government-wide challenges.

These Reviews have led to substantial improvements, both at individual agencies and within the Federal Government overall. FY 2015 accomplishments include:

- Accelerating agency progress toward implementing the use of Strong Authentication PIV cards and tightening policies and practices for privileged users.
- Ensuring that agencies developed incident response plans to improve their ability to respond to cyber incidents.
- Identifying challenges that prevented some agencies from mitigating critical vulnerabilities on their systems in a timely manner and developing action plans to resolve those challenges.
- Resolving governance challenges to ensure all IT organizations within Federal departments work with the department-level Chief Information Officer (CIO) and Chief Information Security Officer on cybersecurity improvements.

These efforts helped to dramatically accelerate progress on key areas of cybersecurity across the Federal Government. In FY 2016, OMB Cyber will leverage increased resources to further expand the CyberStat Review process.

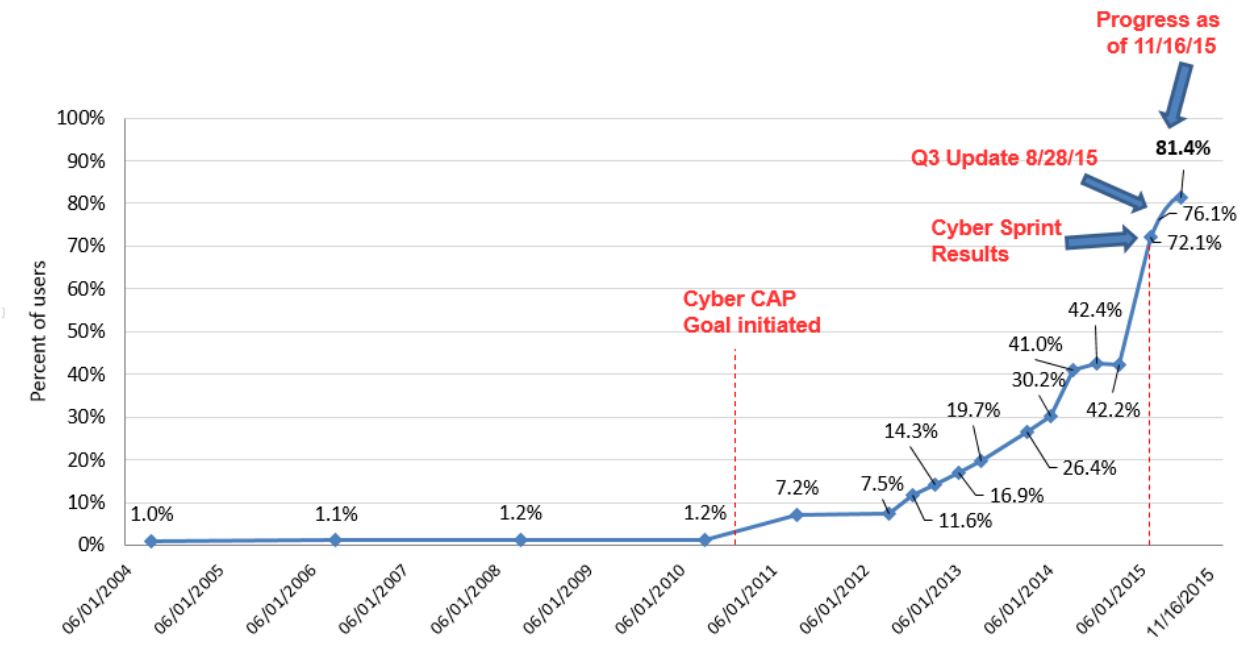
C. 30-DAY CYBERSECURITY SPRINT

In June 2015, the Federal Chief Information Officer launched a 30-day Cybersecurity Sprint to dramatically improve Federal cybersecurity and protect systems against evolving threats. The Cybersecurity Sprint demonstrated that agencies can rapidly identify and close critical gaps resulting in marked improvements to Federal cybersecurity. As part of this initiative, the OFCIO directed agencies to take four high-priority actions to improve their cybersecurity posture:

1. Immediately deploy indicators provided by DHS regarding priority threat-actor techniques, tactics, and procedures to scan systems and check logs;
2. Patch critical vulnerabilities without delay;
3. Tighten policies and practices for privileged users; and,
4. Dramatically accelerate implementation of multi-factor authentication, especially for privileged users.

Agencies made progress in a number of areas during the course of the Cybersecurity Sprint. For example, as shown in **Figure 1**, during the Cybersecurity Sprint, and in accordance with *Homeland Security Presidential Directive 12 (HSPD-12)*, Federal civilian agencies increased their use of Strong Authentication for all users from 42% to 72%, an overall increase of 30%. As of November 16, 2015, Federal civilian agencies had further increased their use of PIV to 81%. This percentage increases to 83% when including the Department of Defense (DOD).

Figure 1: Civilian CFO Act Agency PIV Implementation

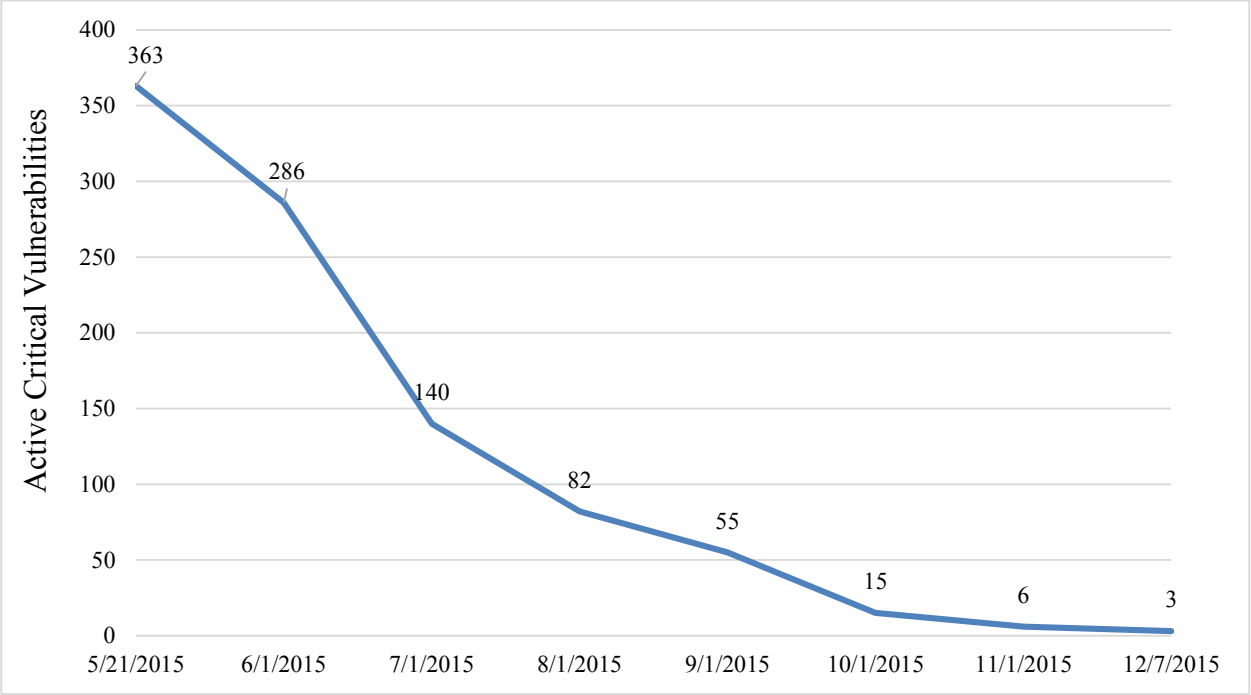


Source: FISMA Data Agency Level Questions submitted to CyberScope and OMB High Priorities Actions Dashboard.
***Note:** DOD is excluded due to the large number of users.

Another Cybersecurity Sprint-related highlight was the accelerated implementation of DHS Binding Operational Directive (BOD) 15-01, issued on May 21, 2015, to mitigate critical vulnerabilities identified by the DHS National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC conducts persistent network and vulnerability scans of all Federal civilian agency internet-accessible systems to identify known critical vulnerabilities and configuration errors, capturing the total number of critical vulnerabilities in a weekly "Cyber Hygiene Report." Because critical vulnerabilities are typically remotely exploitable, have a low complexity to execute, utilize default or no authentication, and impact the confidentiality, integrity, and availability of systems, BOD 15-01 requires all Federal civilian agencies to patch vulnerabilities within 30 days of receiving the NCCIC report. Agencies that are unable to accomplish this must provide a detailed justification to DHS within the same 30-day period outlining any barriers, planned steps for resolution, and a timeframe for mitigation.

As shown in **Figure 2,** prior to the issuance of the BOD, there were 363 known active critical vulnerabilities on Federal systems. OMB and DHS worked with agencies during and after the Cybersecurity Sprint to reduce the number of critical vulnerabilities to three by December 2015, a 99% reduction since the beginning of the initiative.

Figure 2: BOD 15-01: Reduction in Active Critical Vulnerabilities



Source: DHS Binding Operational Directive 15-01 Scorecards May 21, 2015-November 16, 2015

The NCCIC's efforts are ongoing, and new critical vulnerabilities that must be addressed by Federal departments and agencies are identified on an ongoing basis. Given this, the number of active critical vulnerabilities sometimes fluctuates, often rising briefly as agencies work to mitigate newly announced vulnerabilities.

Other highlights associated with the Cybersecurity Sprint include:

- 100% of CFO Act agencies completed Indicators of Compromise scans by July 31, 2015.
- 100% of CFO Act agencies identified their High Value Assets.
- 96% (23 of 24 CFO Act agencies) finished their privileged user reviews by August 31, 2015.

Lastly, as part of the Cybersecurity Sprint, OMB formed an interagency Sprint Team comprised of over 100 cybersecurity professionals from civilian, military, and intelligence agencies. The Sprint Team led a review of Federal cybersecurity policies, procedures, and practices to identify gaps and develop a strategy and action plan for rapid improvement. The Sprint Team's findings served as the basis for the Cybersecurity Strategy Implementation Plan (CSIP), which, as described below, is a detailed strategy and implementation plan dedicated to addressing Federal civilian cybersecurity. OMB expects that agencies will continue to improve their security and track their outcomes across the four objectives highlighted in the CSIP.

D. CYBERSECURITY STRATEGY AND IMPLEMENTATION PLAN (CSIP)

As described in *OMB Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,"* the CSIP is the result of a comprehensive review conducted during the Cybersecurity Sprint, which identified critical cybersecurity gaps and emerging priorities and articulated specific actions to address those gaps and priorities as quickly as possible. The CSIP focuses on strengthening Federal civilian cybersecurity through five objectives:

1. Prioritized identification and protection of high-value assets and information;
2. Timely detection and rapid response to cyber incidents;
3. Rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Cybersecurity Sprint assessment;
4. Recruitment and retention of the most highly-qualified cybersecurity workforce talent the Federal Government can bring to bear; and,
5. Efficient and effective acquisition and deployment of existing and emerging technology.

The CSIP acknowledges the current landscape of Federal cybersecurity by emphasizing the need for a "defense in depth" approach, which relies on the layering of people, processes, technologies, and operations to achieve more secure Federal information systems. The CNAP incorporates all of the CSIP initiatives and includes new actions to drastically improve Federal agencies' cybersecurity. OMB will work with agencies throughout FY 2016 and FY 2017 to implement the CNAP initiatives and track progress and outcomes across the plan's objectives.

E. FY 2015 Policy Updates

In accordance with FISMA, OMB updated relevant guidance on cybersecurity to ensure Federal agencies have best practices and techniques at their disposal. In FY 2016, OMB will establish or update other policies in areas such as security in acquisitions, identity management for government employees, and mobile security. A summary of the policy updates made in FY 2015 is provided below.

OMB Memorandum M-15-13

OMB Memorandum M-15-13, "Policy to Require Secure Connections across Federal Websites and Web Services," issued by OMB on June 8, 2015, requires agencies to secure all their publicly accessible Federal websites and web services with Hypertext Transfer Protocol Secure (HTTPS). The majority of Federal websites use Hypertext Transfer Protocol (HTTP) as the primary protocol to communicate over the public internet. Unencrypted HTTP does not protect data from interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data. Unencrypted HTTP connections also create a privacy vulnerability and expose potentially sensitive information about the users of unencrypted Federal websites and services. HTTPS verifies the identity of a website or web service for a connecting client, and encrypts nearly all information sent between the website or service and the user. OMB M-15-13 seeks to prevent sensitive information from being intercepted or changed while in transit. Per the memorandum, agencies are required to make all existing websites and services accessible through a secure connection (i.e. HTTPS-only) by December 31, 2016. The OFCIO established a public dashboard at *https://www.pulse.cio.gov* to monitor agency compliance with OMB M-15-13. As of January 30, 2016, 39% of Federal Government domains used HTTPS. OMB will continue working with agencies to achieve the requirement laid out in the memorandum.

Data Breach Notification Policies and Procedures

FISMA Section 3553(c) requires OMB, in consultation with DHS, to provide a description of the threshold for reporting major information security incidents and an assessment of agency compliance with data breach notification policies and procedures. Additionally, FISMA Section 3558(b) requires OMB to develop guidance on what constitutes a major incident. OMB addressed these requirements in *OMB Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Regulations*, issued on October 30, 2015. In determining whether a major incident has occurred, OMB M-16-03 directed agencies to consider whether the incident:

1. Involves information that is Classified or may be found listed in the Controlled Unclassified Registry available online at https://www.archives.gov/cui[3];
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.[4]

Since the issuance of OMB M-16-03, no Federal agency has reported a major incident to OMB. OMB will continue to monitor agencies' compliance with OMB M-16-03 and report on major incidents in future annual reports to Congress.

Revisions to OMB Circular A-130

FISMA Section 3558(f) requires OMB to amend or revise *OMB Circular A-130, "Managing Information as a Strategic Resource,"* (the Circular) in order to eliminate inefficient and wasteful reporting. While OMB routinely releases policies and guidance to address specific challenges faced by Federal agencies, the Circular serves as the overarching policy that provides guidance on how agencies should manage Federal information resources. OMB has begun the process of significantly revising the Circular to bring it up-to-date with current statute, policy, and practices. In the process of developing new language and provisions for the Circular, OMB asked for public comment on proposed guidance and conducted extensive outreach efforts to engage stakeholders within, and external to, the Government.

The proposed Circular reflects a rapidly evolving digital economy where more than ever, individuals, groups, and organizations rely on IT to carry out a wide range of missions and business functions. IT changes rapidly and the Federal workforce managing IT must have the flexibility to address known and emerging threats while implementing continuous improvements. This update acknowledges the pace of change and the need to increase capabilities provided by 21st century technology while recognizing the need for strong governance and safeguarding of taxpayer funded assets and information.

F. BUILDING A SUSTAINABLE FEDERAL CYBERSECURITY WORKFORCE

The Federal Government suffers from a shortage of cybersecurity professionals due to persistent recruitment and retention challenges. The FY 2015 Cybersecurity Sprint identified two key observations related to the Federal cybersecurity workforce:

1. The vast majority of Federal agencies cite a lack of cyber and IT talent as a major resource constraint that impacts their ability to protect information and assets.
2. There are a number of existing Federal initiatives to address this challenge, but implementation and awareness of these programs is inconsistent.

To harmonize existing work streams and identify new initiatives to enhance recruitment and retention, the CSIP initiated an effort to compile a Cybersecurity Human Resources Strategy by the end of April 2016. Additionally, during FY 2015 OMB collaborated with workforce experts from across the Federal Government to implement the CSIP workforce initiatives, which resulted in:

- The Office of Personnel Management (OPM) and OMB issuing a compilation of existing Special Hiring Authorities that can be used to hire cybersecurity and IT professionals across the Federal Government.
- DHS launching a pilot of the Automated Cybersecurity Position Description Hiring Tool across the Federal Government.
- OPM, DHS, and OMB mapping the entire cyber workforce landscape across all agencies using the National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework, and identifying cyber talent gaps and recommendations for closing those gaps.
- OPM, DHS, and OMB developing recommendations for Federal workforce training and professional development in functional areas outside of cybersecurity and information technology that support cybersecurity efforts.

The CNAP builds on the CSIP by incorporating all of these activities and detailing new initiatives to enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure Federal agencies. The CNAP initiatives include:

- Establishing a Cybersecurity Reserve, which is a cadre of cybersecurity experts that the Federal Government can call upon to rapidly respond to cybersecurity challenges;
- Developing a foundation cybersecurity curriculum for academic institutions to consult and adopt; and,
- Providing grants to academic institutions to develop or expand cyber education programs as part of the National Centers of Academic Excellence in Cybersecurity Program.

Several Federal agencies, including OPM, DHS, the National Science Foundation, the National Security Agency, and the National Initiative for Cybersecurity Education within the National Institute of Standards and Technology (NIST) are already leading a series of nationwide efforts to address ongoing recruitment and retention challenges. Throughout FY 2016 and FY 2017, OMB will continue to work with these agencies to implement the CNAP initiatives and enhance existing programs that help ensure the Federal Government can recruit, develop, and maintain the workforce necessary to defend Federal systems, networks, and data.

G. FEDERAL GOVERNMENT PROGRAMS DESIGNED TO COMBAT GROWING THREATS

The Federal Government relies on a variety of initiatives to ensure the continued protection of Federal information and information systems. First, FISMA requires agencies to maintain an information security program commensurate with their risk profile. For instance, agencies are responsible for assessing and authorizing information systems to operate within their own networks and for determining which users have the authority to access agency information. Second, DHS is the operational lead for Federal civilian cybersecurity, and executes a number of protection programs on behalf of the Federal Government. Third, NIST issues and updates security standards for information systems utilized by Federal agencies. Finally, OMB, in partnership with NSC and DHS, oversees the successful implementation of agency-specific and government-wide cybersecurity programs. The remainder of Section II highlights some of the critical government-wide cybersecurity programs and initiatives administered by DHS and other Federal agencies.

Continuous Diagnostics and Mitigation (CDM)

Per *OMB Memorandum 14-03, "Ensuring the Security of Federal Information and Information Systems,"* DHS operates the CDM program in partnership with OMB. Under CDM, DHS works with the General Services Administration (GSA) to establish and fund government-wide blanket purchase agreements that provide Federal agencies a basic set of tools to support the continuous monitoring of information systems. These tools include agency dashboards with customizable report functions and a Federal enterprise-wide dashboard that will allow DHS to improve its response to cyber threats. Once fully implemented, CDM will enable agencies to identify and respond to cybersecurity challenges in near real-time.

DHS is implementing CDM in multiple phases, each designed to allow agencies to implement the tools and services in a consistent manner that demonstrates measureable cybersecurity results and leverages strategic sourcing to achieve cost savings. Phase One of CDM focuses on endpoint integrity and device management. Specifically, this phase encompasses the management of hardware and software assets, configuration management, and vulnerability management. These capabilities form an essential foundation on which the rest of CDM will build.

In FY 2014, through an order valued at $59.5 million, the program delivered over 1.7 million licenses for these security monitoring tools and products to agencies. This marked a major step in the implementation of CDM and demonstrated the efficiency of the blanket purchase agreements resulting in $26 million in cost avoidance when compared to the GSA Schedule. By the end of FY 2015, CDM awarded five additional contracts to provide Phase One tools, sensors, dashboards, and integration services to the 23 civilian CFO Act agencies. The total contract award values were $205 million, which DHS estimates achieved a savings of $142 million off the GSA Schedule, approximately 41% in cost savings. With these awards, the program now provides 97% of the Federal civilian workforce with endpoint management tools.

The program is actively planning to deliver Phase Two tools and sensors to agencies in FY 2016. Phase Two focuses on monitoring attributes of authorized users operating in an agency's computing environment. These attributes include the individual's security clearance or suitability, security related training, and any privileged access they may possess. Phase Three of the program will focus on boundary protection and response to cyber incidents and vulnerabilities. These capabilities will include audit and event detection and response, status of encryption, remote access, and access control of the environment. Additionally, the FY 2017 President's Budget invests additional funds to accelerate and enhance CDM implementation, with the long-term goal of increasing common cybersecurity platforms and services that

protect Federal civilian Government as a holistic enterprise.

National Cybersecurity Protection System (EINSTEIN)

The goal of the National Cybersecurity Protection System (operationally known as EINSTEIN) is to provide the Federal Government with an early warning system, improved situational awareness of intrusion threats to Federal Executive Branch civilian networks, as well as 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 (E³A) in 2012, which 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 E³A focused on countermeasures that address approximately 85% of the cybersecurity threats affecting Federal civilian networks.

To date, E³A provides services to approximately 49% of the Federal civilian user base, representing approximately 1.1 million users. DHS initially projected it would be able to offer E³A protection capabilities to all civilian CFO Act agencies by the end of calendar year 2018; however, due to accelerated deployment efforts, DHS now projects it will offer E³A to all civilian CFO Act agencies by the end of calendar year 2016. DHS also began rolling out an E³A Service Extension to agencies with internet service providers that do not offer E³A protections. The E³A Service Extension allows those agencies to send their traffic through E³A sensors to receive the same countermeasures. DHS will continue to progress and build on the accomplishments of FY 2015 to provide advanced intrusion detection and prevention capabilities for Federal systems.

Facilitating Mobile Security

Smart phones have become ubiquitous and indispensable for consumers and businesses alike. Although these devices are relatively small and inexpensive, they provide services for voice calls, simple text messages, sending and receiving e-mails, browsing the web, online banking and e-commerce, social networking, and many functions once limited to laptop and desktop computers. Smart phones and tablet devices have specialized built-in hardware, such as photographic cameras, video cameras, accelerometers, Global Positioning System receivers, and removable media readers. They also employ a wide range of wireless interfaces, including infrared, Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Communications, and one or more types of cellular interfaces that provide network connectivity across the globe. Government agencies can achieve productivity gains in much the same way as consumers and businesses using these technologies.

As with any new technology, smart phones provide new capabilities, but also pose a number of new security and privacy challenges. For example, new capabilities enabled by smart phones are only helpful if they are used by the appropriate person with the appropriate credentials. This challenge is well known, but existing solutions for Strong Authentication, such as a smart card reader for PIV cards, have not been user-friendly or have been too expensive to adopt agency-wide. As the pace of the technology life cycles continues to increase, current information assurance standards and processes must be updated to allow government users to employ the latest technologies without diminishing privacy and security.

With these concerns in mind, during FY 2015, NIST published *Special Publication (SP) 800-163, "Vetting the Security of Mobile Applications*," along with open source test code and guidance for constructing a mobile application-testing program. The guidelines describe vulnerabilities and poor

programming practices for both Android and iOS devices, which entities can mitigate through other described security technologies.

This publication also helps government agencies perform security and privacy assessments on mobile apps. The purpose of this work is to help organizations:

- Understand the process for vetting the security of mobile applications;
- Plan for the implementation of an app vetting process;
- Develop app security requirements;
- Understand the types of app vulnerabilities and the testing methods used to detect those vulnerabilities; and,
- Determine if an app is acceptable for deployment on the organization's mobile devices.

NIST also addressed the issue of Strong Authentication with mobile devices through the release of *SP 800-157, "Guidelines for Derived Personal Identity Verification Credentials."* In addition to these standards, the National Cybersecurity Center of Excellence at NIST created a draft building block on how to implement derived credentials for a specific use case. Agencies are currently piloting the use of derived credentials. The National Cybersecurity Center of Excellence will continue to develop the building block in FY 2016 to assist agencies with implementation of Strong Authentication for mobile devices.

FedRAMP and the Safe, Secure Adoption of Cloud

To accelerate the adoption of cloud computing solutions across the Federal Government, the OFCIO published "*Security Authorization of Information Systems in Cloud Computing Environments*" on December 8, 2011. This memorandum announced the establishment of the *Federal Risk and Authorization Management Program (FedRAMP),* a process that replaced the varied and duplicative cloud service assessment procedures across government by providing agencies with a standard approach. FedRAMP provides agencies with a standardized approach to the security assessment, authorization, and continuous monitoring of cloud services in accordance with FISMA by:

- Standardizing security requirements for government-procured cloud solutions;
- Reducing duplicative efforts, inconsistencies, and cost inefficiencies; and,
- Enabling the Federal Government to accelerate the adoption of cloud computing.

There are two primary tracks for agencies to authorize FedRAMP compliant cloud services: Agency-level authorizations and Joint Authorization Board (JAB) authorizations. Under the agency-level authorization track, agencies can work directly with a Cloud Service Provider (CSP) to sponsor and issue an Authority to Operate (ATO). Once the FedRAMP Program Management Office validates the sponsoring agency's ATO as FedRAMP compliant, other agencies can reuse the security package to issue their own authorization to a CSP. Agencies, however, seeking to leverage an existing ATO package sponsored by another agency must still issue their own ATO. Under the JAB Provisional Authorization path CSPs can independently submit security packages for review by the JAB, which is composed of the CIOs of DHS, the DOD, and GSA. The FedRAMP Program Management Office and the JAB conduct a rigorous technical review of these packages. If approved, the JAB issues a Provisional Authorization to Operate, though the JAB does not accept risk on behalf of any agency. Agencies can access Provisional Authorization packages and reuse them to make their own risk-based decision in issuing their own ATO.

In FY 2015, agencies accredited 86 CSPs as FedRAMP compliant ATOs (including both JAB Provisional ATOs and Agency ATOs). Of these 86, 50 were issued by agencies (20 original agency

authorizations for CSPs and 30 ATOs that relied on the reuse of other-agency security packages). The JAB issued Provisional ATOs to 13 CSPs, which were re-used by agencies to authorize an additional 23 ATOs.

In FY 2015, OMB and GSA identified strategies to improve the program's effectiveness, efficiency, and transparency to ensure the FedRAMP model continues to evolve and scale. OMB and GSA worked collaboratively to clarify program requirements, improve the quality of data available to bolster the ability of agencies to reuse packages, simplify the JAB Provisional Authorization process, and scale the agency ATO process to keep pace with increasing demand. OMB and GSA will continue this work in FY 2016 to strengthen FedRAMP and ensure this vital program continues to support agencies' ability to adopt secure cloud solutions in an agile, secure, and efficient manner.

SECTION II: FEDERAL CYBERSECURITY PERFORMANCE

During FY 2015, the Federal Government saw an increase in the number of information security incidents affecting the integrity, confidentiality, and/or availability of government information, systems, and services. The data reported by agencies to the United States Computer Emergency Readiness Team (US-CERT) enables OMB and DHS to analyze areas of vulnerability and determine where improved defenses appear to have had a positive impact. This section identifies cybersecurity incident information reported by agencies to US-CERT in FY 2015. It also provides a review of agency performance against initiatives developed to address cybersecurity challenges. **Appendix 2: FY 2015 Cybersecurity CAP Metrics** contains additional information on agency performance against cybersecurity initiatives and metrics.

A. FY 2015 CYBERSECURITY INCIDENT REPORTING

In accordance with FISMA Section 3556, US-CERT, which resides within DHS, serves as the Federal information security incident center. US-CERT uses the NIST *SP 800-61 Rev 2, "Computer Security Incident Handling Guide"* definition of a computer security incident, which is as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Pursuant to FISMA Section 3554, each Federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems managed by a Federal agency, contractor, or other source which supports the operations and assets of the agency.

As seen in Table 1, the number of incidents has increased over the past three years. In FY 2015, agencies reported 77,183 incidents to US-CERT, which is a 10% increase over the 69,851 incidents reported in FY 2014. The overall rise in the number of incidents represents both an increase in total information security events and agencies' enhanced capabilities to identify, detect, manage, respond to, and recover from these incidents. **Table 1** shows the total number of cybersecurity incidents reported by CFO Act and non-CFO Act small agencies to US-CERT. **Appendix 1** of this report provides the agency-specific data for each CFO Act agency.

Table 1: Federal Agency Incidents Reported to US-CERT in FY 2013 - FY 2015

Reporting Source	FY 2013 Total Number of Incident Reports	FY 2014 Total Number of Incident Reports	FY 2015 Total Number of Incident Reports
CFO Act Agencies	57,971	67,196	75,087
Non-CFO Act Agencies	2,782	2,655	2,096
Total Federal Incidents	**60,753**	**69,851**	**77,183**

Source: Data reported to US-CERT Incident Reporting System from October 1, 2012, to September 30, 2015.
Note: The incident data used for this table and the figures below excludes agency exercises and network testing, requests for information, and Joint Indicator Bulletins as these items are not actual information security incidents. The data also excludes cases where key data fields, such as agency, sub-agency, and the incident category were not included or left blank in the submission.

US-CERT developed incident reporting guidelines for agencies to use when reporting security incidents. These guidelines were revised in FY 2015 to improve the data US-CERT received from agencies. The primary focus of the legacy incident reporting category system—last updated by US-CERT in 2007—was incident categorization and identification of the root cause, which caused delays in notification and provided limited data regarding the impact of incidents. To address these issues and assist in the execution of its mission objectives, US-CERT issued new reporting guidelines in FY 2015, which provide for:

- Greater quality of information - Alignment with incident reporting and handling guidance from NIST SP 800-61 Rev. 2 to introduce functional, informational, and recoverability impact classifications, allowing US-CERT to better recognize significant incidents;
- Improved information sharing and situational awareness - Establishing a one-hour notification time frame for all incidents with a confirmed impact to confidentiality, integrity, or availability to improve US-CERT's ability to understand cybersecurity events affecting the government; and,
- Faster incident response times - Moving causal analysis to the closing phase of the incident handling process to expedite initial notification.

The new guidelines became effective October 1, 2014; however, in order to allow time for Federal agencies to transition to the new reporting system, agencies were able to continue reporting incidents using the legacy incident reporting category system until September 30, 2015. This report to Congress only identifies incidents using data from the legacy system, as agencies were transitioning to the new reporting system throughout FY 2015. As of October 1, 2015, all CFO agencies are reporting incidents using the new incident notification guidelines. OMB and US-CERT will continue to work with agencies as they utilize the new guidance. In future annual reports, OMB and US-CERT will be able to include information regarding the functional and informational impact of incidents as well as the recoverability from those incidents.

Table 2 provides definitions for all types of computer security incidents. Although US-CERT issued new reporting guidelines in FY 2015, the definitions shown in this table did not change. Readers should note that this table includes both computer security incident categories as well as selected subcategories. The table notes distinguishable subcategories along with the larger category to which they belong.

Table 2: US-CERT Incident Definitions

Category/Subcategories	Definition
Denial of Service (DoS)	This category is used for all *successful* DoS incidents, such as a flood of traffic, which renders a web server unavailable to legitimate users.
Improper Usage	Improper Usage categorizes all incidents where a user violates acceptable computing policies or rules of behavior. These include incidents like the spillage of information from one classification level to another.
-Unauthorized Access	Unauthorized Access is when individual gains logical or physical access without permission to a Federal agency network, system, application, data or other resource. (*Subcategory of Improper Usage Category*)
-Social Engineering	Social Engineering is used to categorize fraudulent web sites and other attempts to entice users to provide sensitive information or download malicious code. Phishing is a set of Social Engineering, which is itself a subcategory of Unauthorized Access. (*Set of Unauthorized Access Subcategory*)
-Phishing	Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques, typically via emails containing links to fraudulent websites. (*Set of Social Engineering Subcategory*)
-Equipment	This set of Unauthorized Access is used for all incidents involving lost, stolen or confiscated equipment, including mobile devices, laptops, backup disks or removable media. (*Set of Unauthorized Access Subcategory*)
-Policy Violation	Policy Violation is primarily used to categorize incidents of mishandling data in storage or transit, such as digital personally identifiable information (PII) records or procurement sensitive information found unsecured or PII being emailed without proper encryption. (*Subcategory of Improper Usage Category*)
Malicious Code	Used for all *successful* executions or installations of malicious software, which are not immediately quarantined and cleaned by preventative measures such as antivirus tools.
Non-Cyber	Non-Cyber is used for filing all reports of PII spillages or possible mishandling of PII, which involve hard copies or printed material as opposed to digital records.
Other	For the purposes of this report, a separate superset of multiple subcategories has been employed to accommodate several low-frequency types of incident reports, such as unconfirmed third-party notifications, failed brute force attempts, port scans, or reported incidents where the cause is unknown.
Suspicious Network Activity	This category is primarily utilized for incident reports and notifications created from EINSTEIN data analyzed by US-CERT.

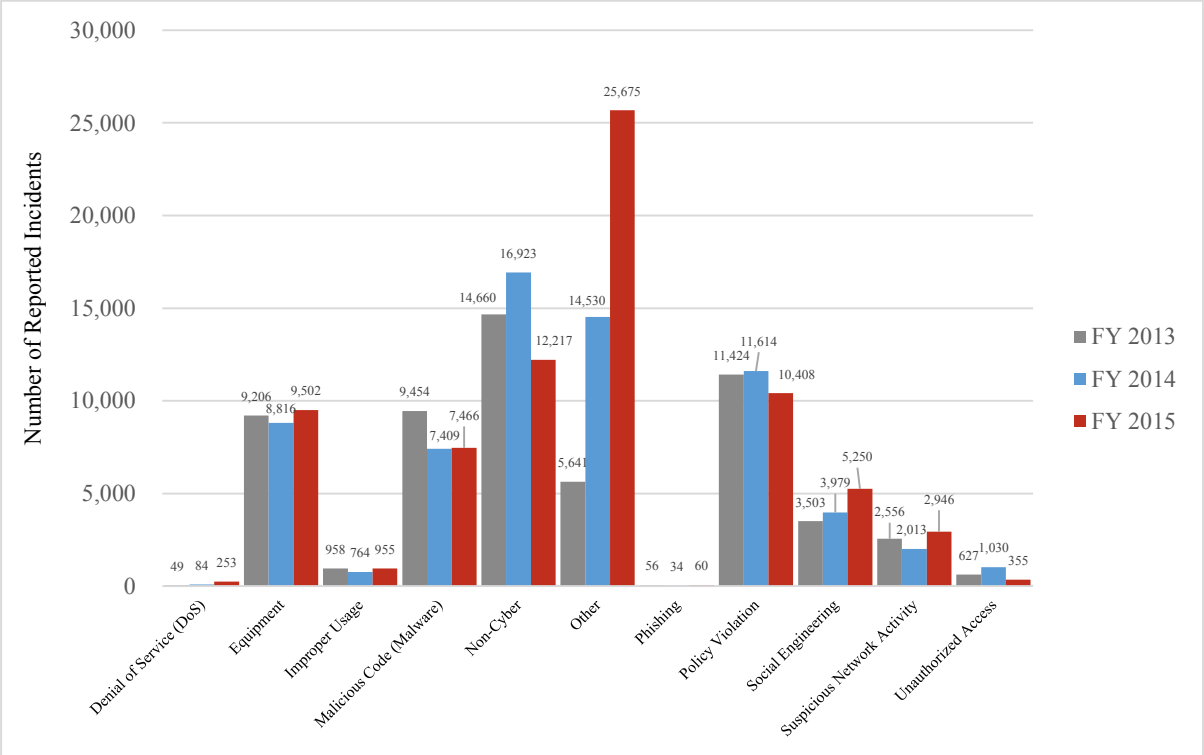
Source: Definitions are provided by US-CERT and are available at *https://www.us-cert.gov/government-users/reporting-requirements.*

CFO Act Agency Incidents Reported to US-CERT

Figure 3 identifies cybersecurity incident information reported by agencies to US-CERT. As shown in **Figure 3**, US-CERT processed 75,087 incidents reported by CFO Act agencies in FY 2015. The 'Other' category comprises 25,675 incidents, which represents 34% of all incidents reported in FY 2015, a nearly 77% increase in that category of incident from what was reported in FY 2014. This category includes incidents such as scans, probes and attempted access, incidents under investigation, and incidents categorized as miscellaneous. Approximately 59% of 'Other' incidents fall within the attempted access subcategory due to the high volume of scans and probes.

Figure 3 also shows the second most reported category was Non-Cyber, which includes incidents involving the mishandling of sensitive information without a cybersecurity component, such as the loss of hard copy PII records. This category represented 12,217, or 16% of reported incidents. The third most reported category was Policy Violations, which represent 10,408 reported incidents, or 14% of total incidents reported.

Figure 3: Summary of CFO Act Agency Incidents Reported to US-CERT FY 2013 - FY 2015



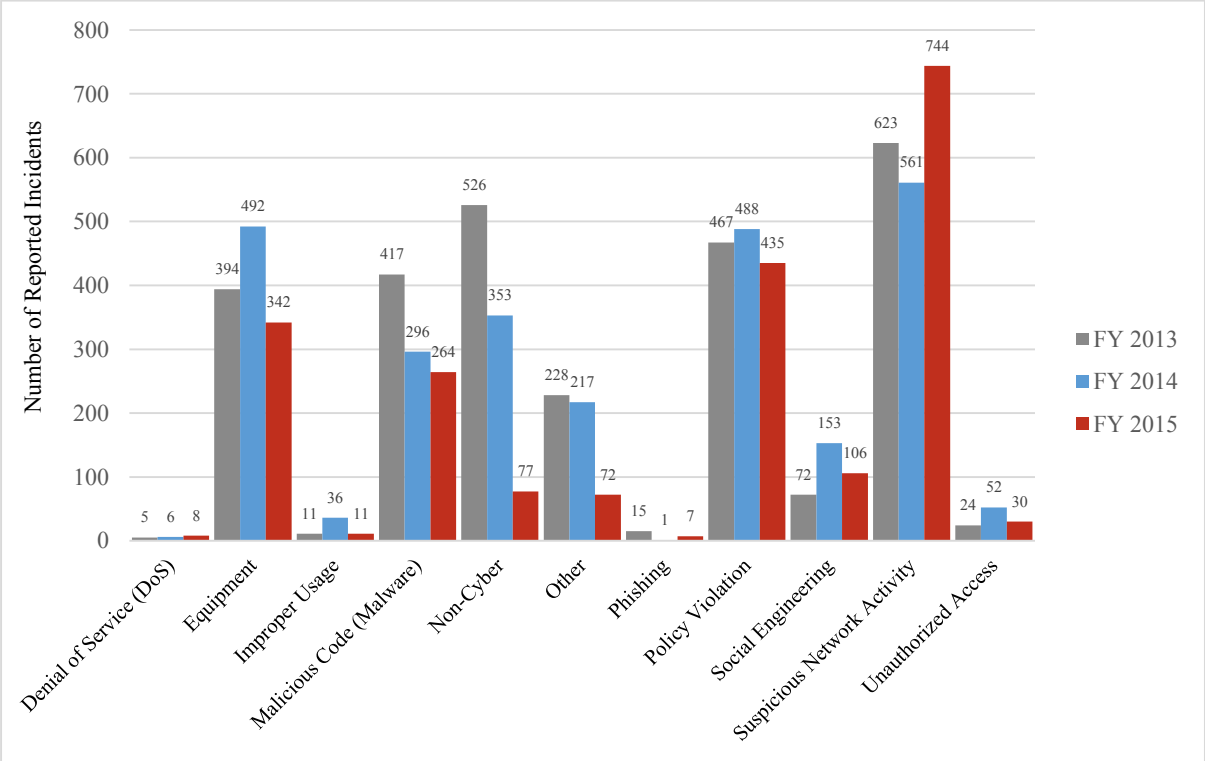
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2015.

While phishing attempts continue to be a primary method for exploiting Federal systems and data, US-CERT's incident categories, depicted in **Figure 3**, do not capture the magnitude of this threat. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send an email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. Although Federal agencies categorize these as phishing incidents, US-CERT categorizes these incidents based on the root cause, such as malicious code or social engineering, rather than the source. For this reason, **Figure 3** shows a low number of phishing incidents compared to the high number of malicious code and social engineering incidents.

Non-CFO Act Agency Incidents Reported to US-CERT

Figure 4 identifies cybersecurity incident information reported by non-CFO Act agencies to US-CERT. During FY 2015, US-CERT processed 2,096 incidents reported by non-CFO Act agencies. As shown in **Figure 4**, Suspicious Network Activity was the largest category of incidents reported by these agencies in FY 2015. This category represented 744 incidents, or 35%, of reported incidents. This category is primarily comprised of incident reports and notifications created from EINSTEIN data. The second most frequently reported incident type was Policy Violations. This category includes the mishandling of data storage and transmission, with 435 reported incidents, or 21% of total incidents. The third most frequently reported incident category in FY 2015 was Equipment. This category includes all incidents involving lost, stolen or confiscated equipment, including mobile devices, laptops, backup disks or removable media. Agencies reported 342 incidents, or 16% of total incidents, in this category.

Figure 4: Summary of Non-CFO Act Agency Incidents Reported to US-CERT in FY 2013-FY 2015



Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2015.

B. AGENCY CYBERSECURITY CROSS AGENCY PRIORITY (CAP) GOAL PERFORMANCE

Recognizing the continued risk that cybersecurity incidents pose to Federal information and information systems, OMB, in coordination with NSC, DOD, and DHS, developed a new *Cybersecurity CAP goal* for FY 2015 through FY 2017. The Cybersecurity CAP goal represents a basic building block of a strong cybersecurity program as it establishes a minimum threshold for agencies to secure their information technology enterprise. The CAP goal improves awareness of security practices, vulnerabilities, and addresses threats to the operating environment by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity. The FY 2015-FY 2017 Cybersecurity CAP goal is comprised of the following three priority areas:

- **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.

- **Identity, Credential, and Access Management (ICAM/Strong Authentication)** – The goal of Strong Authentication is to implement a set of capabilities that ensure users must authenticate to Federal IT resources and have access to only those resources that are required for their job function. Updated Strong Authentication metrics allow OMB and DHS to better identify and protect access to Federal information assets.

- **Anti-Phishing and Malware Defense** – This is a new initiative for FY 2015-FY 2017. The goal of Anti-phishing and Malware Defense is to implement technologies, processes, and training that reduce the risk of malware introduced through email and malicious or compromised web sites.

The FY 2015-FY 2017 CAP goal breaks the three priority areas into sub-components. The ISCM sub-component consists of hardware asset management, software asset management, secure configuration management, and vulnerability management. The ICAM sub-component now consists of both unprivileged user PIV and privileged user PIV usage. Finally, the Anti-Phishing and Malware Defense sub-component, a new priority area, consists of Anti-Phishing Defense, Malware Defense, and Other Defense. The metrics within these sub-components are more refined than in previous years and better enable OMB, DHS, and agency leadership to measure agency performance with increased specificity.

The following tables provide an overview of performance across the FY 2015-FY 2017 Cybersecurity CAP goal priority areas. Due to changes to the ISCM metrics and the addition of the Anti-Phishing and Malware Defense metrics, trending performance over time is not possible across all initiatives. Where possible, the tables below provide a comparison of FY 2014 and FY 2015 performance data. The tables also rank CFO Act agency performance against these cybersecurity CAP goals from the highest performing to the lowest performing for each cybersecurity capability component.

The ISCM Hardware Asset Management metric provides data on an agency's ability to detect devices on an organization's unclassified network. As seen in **Table 3**, ten agencies met the 95% or greater target in both 'Capability to Detect Unauthorized Hardware' and 'Automated Enterprise-level Visibility Capability' metrics. The gray cells in the table indicate agencies that did not meet this target.

Table 3: ISCM Hardware Asset Management Capabilities FY 2015

Agency	Capability to Detect Unauthorized Hardware Assets (%)	Automated Enterprise-level Visibility Capability (%)
National Science Foundation (NSF)	100	100
Nuclear Regulatory Commission (NRC)	100	100
Office of Personnel Management (OPM)	100	100
Social Security Administration (SSA)	100	100
Department of Labor (Labor)	99	100
Department of Transportation (DOT)	99	100
Small Business Administration (SBA)	98	99
Department of Justice (Justice)	97	97
U.S. Agency for International Development (USAID)	96	95
Department of Agriculture (USDA)	95	98
Department of Defense (DOD)	93	83
Department of Health and Human Services (HHS)	92	94
Department of Energy (Energy)	89	87
Department of the Treasury (Treasury)	83	100
Department of State (State)	81	100
Department of Education (ED)	77	100
General Services Administration (GSA)	73	100
Department of Commerce (Commerce)	66	85
Department of Housing and Urban Development (HUD)	62	91
Department of Homeland Security (DHS)	54	97
Department of the Interior (Interior)	46	89
Environmental Protection Agency (EPA)	2	64
Department of Veterans Affairs (VA)	0	94
National Aeronautics and Space Administration (NASA)	0	93
CFO Act Agency Average*	72	90

Source: Analysis of FISMA Agency Level Questions Data (Questions 2.2, 2.3) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015. See *www.performance.gov* for FY 2015 Q1-Q4 information.

*__Note:__ This is a weighted average based on the total number of hardware assets connected to the agencies' unclassified network(s).

The ISCM Software Asset Management metric provides data on an agency's ability to automatically detect software and block unauthorized software from executing. Seven agencies met the 95% or greater target in both Automated Software Asset Inventory and Capability to Block and Detect Unauthorized Software metrics. As seen in **Table 4**, 17 of the 24 CFO Act agencies have achieved the CAP goal target of 95% for Automated Software Asset Inventory. However, due to the number of endpoints at some of the lower scoring agencies, the government-wide average is only 89%. Agencies did not perform as well on the Capability to Block and Detect Unauthorized Software metric, with only seven agencies achieving the 95% target score and a government-wide average of only 68%. The gray cells in the table indicate agencies that did not meet this target.

Table 4: ISCM Software Asset Management Capabilities FY 2015

Agency	Automated Software Asset Inventory Capability (%)	Capability to Detect and Block Unauthorized Software (%)
USDA	100	100
ED	100	17
HUD	100	0
Labor	100	96
DOT	100	90
NSF	100	0
OPM	100	100
SSA	100	100
Interior	99	57
NRC	99	92
State	98	98
GSA	98	96
SBA	98	2
Justice	97	97
Treasury	96	91
USAID	95	0
Commerce	95	72
VA	91	0
DHS	88	58
DOD	87	82
NASA	83	2
HHS	76	32
EPA	68	67
Energy	67	39
CFO Act Agency Average*	89	68

Source: Analysis of FISMA Agency Level Questions Data (Questions 2.6, 2.7) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

***Note:** This is a weighted average based on the total number of endpoints connected to the agencies' unclassified network(s).

The ISCM Secure Configuration Management metric provides data on the percentage of hardware assets covered by an agency's auditing activities. As seen in **Table 5**, 15 of the 24 CFO Act agencies achieved the CAP goal target of 95%, while three other agencies fell just a few percentage points below the goal. The gray cells in the table indicate agencies that did not meet this target.

Table 5: ISCM Secure Configuration Management Capabilities FY 2015

Agency	Secure Configuration Management (%)
USDA	100
HUD	100
Labor	100
SSA	100
Interior	99
Justice	99
Treasury	99
VA	99
NRC	99
OPM	99
EPA	98
NSF	98
SBA	97
State	95
GSA	95
ED	94
Commerce	91
Energy	91
DHS	87
NASA	86
HHS	75
USAID	75
DOT	21
Civilian CFO Act Agency Average*	92

Source: Analysis of FISMA Agency Level Questions Data (Questions 2.10.1, 2.10.6) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

***Notes:** This is a weighted average based on the total number of agencies' hardware assets in the Top ten list of United States Government operating systems. Additionally, this table excludes data from DOD. DOD reported 0% for this metric in its FY 2015 FISMA report.

The Vulnerability Management metric provides data on the percentage of hardware assets that are assessed using credentialed scans with Security Content Automation Protocol validated vulnerability tools. As seen in **Table 6**, only nine of 24 CFO Act agencies achieved the CAP goal target of 95% for ISCM Vulnerability Management. The gray cells in the table indicate agencies that did not meet this target.

Table 6: ISCM Vulnerability Management Capabilities FY 2015

Agency	Vulnerability Management (%)
SSA	100
USAID	100
Labor	99
SBA	99
Treasury	98
GSA	98
Justice	97
NRC	96
OPM	95
DHS	93
NSF	88
USDA	85
ED	85
HHS	82
State	82
NASA	82
HUD	76
Commerce	74
Interior	68
VA	49
Energy	31
DOT	30
DOD	20
EPA	0
CFO Act Agency Average*	52

Source: Analysis of FISMA Agency Level Questions Data (Question 2.11) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

***Note:** This is a weighted average based on the total number hardware assets connected to the agencies unclassified network(s). DOD reported 20% for this metric in its FY 2015 FISMA report stating that due to a change in reporting tools, many assets were not yet able to report their data to their enterprise-reporting tool

In FY 2014, the Strong Authentication target was 75% for both unprivileged and privileged users. For the first two quarters of FY 2015, the Strong Authentication target was increased to 85% for both unprivileged and privileged users. OMB shifted the privileged users target to 100% as part of the 30-day Cybersecurity Sprint because privileged users possess elevated levels of system access. During the Cybersecurity Sprint, OMB also specified that users' Strong Authentication credentials must provide a Level of Assurance equivalent to NIST Level 4, implemented through use of the PIV card, as detailed in NIST *SP 800-63 Rev. 2, "Electronic Authentication Guideline*." Historically, this number had lagged behind unprivileged user implementation, despite the greater access afforded to these users. However, as seen in **Table 7** below, the CFO Act agencies' privileged user PIV usage increased significantly over the last year, increasing from 32% overall in FY 2014 to 62% in FY 2015. The gray cells in the table indicate agencies that did not meet this target.

Table 7: Strong Authentication Capabilities – Privileged Users - FY 2014 & FY 2015

Agency	Privileged User PIV FY 2014 (%)	Privileged User PIV FY 2015 (%)
HUD	0	100
Interior	16	100
State	0	100
DOT	13	100
Treasury	2	100
VA	0	100
EPA	0	100
GSA	0	100
NASA	1	100
NSF	66	100
OPM	100	100
SBA	0	100
USAID	0	100
DHS	36	99
SSA	99	99
HHS	4	99
NRC	0	97
Labor	0	95
USDA	0	89
Commerce	95	86
Justice	27	65
ED	84	27
Energy	25	7
Civilian CFO Act Agency Average*	25	81
DOD	38	51
All CFO Act Agency Average*	32	62

Source: Analysis of FISMA Data-Agency Level Questions 5.3, 5.4.5 (FY 2014 Q4) and 3.2, 3.2.1 (FY 2015 Q4) reported to DHS via CyberScope from October 1, 2013, to November 16, 2015, and the OMB High Priorities Actions Dashboard.
***Note:** This is a weighted average based on the total number of individuals at the agencies who have privileged network accounts.

In FY 2014, the Strong Authentication target was 75% for both unprivileged and privileged users. For FY 2015, the Strong Authentication target was increased to 85% unprivileged users. As seen in **Table 8**, unprivileged user PIV usage increased significantly over the last year, increasing from 73% in FY 2014 to 84% in FY 2015. The gray cells in the table indicate agencies that did not meet this target.

Table 8: Strong Authentication Capabilities – Unprivileged Users - FY 2014 & FY 2015

Agency	Unprivileged User PIV FY 2014 (%)	Unprivileged User PIV FY 2015 (%)
GSA	100	99
OPM	0	99
DOT	31	97
Treasury	45	97
EPA	75	97
Interior	37	96
DHS	81	95
HUD	0	95
NRC	0	93
Labor	0	92
HHS	73	87
SBA	0	89
NSF	16	87
USDA	6	86
SSA	84	86
Commerce	87	82
VA	10	80
ED	85	78
NASA	84	77
Justice	44	64
State	0	38
USAID	3	35
Energy	29	11
Civilian CFO Act Agency Average*	41	81
DOD	88	86
All CFO Act Agency Average*	73	84

Source: Analysis of FISMA Data-Agency Level Questions 5.1, 5.2.5 (FY 2014 Q4) and 3.1, 3.1.1 (FY 2015 Q4) reported to DHS via CyberScope from October 1, 2013, to November 16, 2015, and the OMB High Priorities Actions Dashboard.
***Note:** This is a weighted average based on the total number of people at the agencies who have unprivileged network accounts.

To ensure that the Cybersecurity CAP goal was adequately capturing agency efforts to implement capabilities in support of the Anti-Phishing and Malware Defense initiative, specific metrics were included into each of the three subcomponent measures that compose it. Agencies were required to achieve 90% for a certain number of the metrics comprising each initiative subcomponent in order to meet the CAP goal target. For Anti-Phishing Defense, agencies had to achieve 90% coverage on five of seven metrics. The percentage seen in **Table 9** represents the lowest percentage implementation of each agency's top-five performing metrics. The right-hand column captures the total number of agency metrics that met the 90% threshold. As seen in **Table 9**, 14 of the 24 CFO Act agencies achieved 90% or greater on at least five of seven metrics (e.g., ensuring that inbound email passes through anti-phishing filtration technology and requiring emails to be digitally signed). The gray cells in the table indicate agencies that did not meet this target.

Table 9: Anti-Phishing Defense FY 2015

Agency	Anti-Phishing Defenses FY 2015 (%)	Number of Metrics Meeting CAP Goal
USDA	100	6
Labor	100	6
VA	100	6
GSA	100	6
SSA	100	6
HUD	95	6
ED	100	5
Interior	100	5
State	100	5
DOT	100	5
OPM	100	5
USAID	96	5
HHS	93	5
NSF	90	5
Treasury	88	4
Justice	71	4
DHS	69	4
NRC	57	4
EPA	0	4
SBA	0	4
Energy	42	3
DOD	15	3
NASA	8	3
Commerce	42	2
CFO Act Agency Average	74	5

Source: Analysis of FISMA Data- Agency Level Questions (Questions 4.2, 4.5, 4.6, 4.7, 4.9, 4.13, 8.2.1) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Similar to the Anti-Phishing Defense metric, agencies had to achieve 90% coverage on three of five metrics making up the Malware Defense initiative to meet the target (e.g., deployment of host-based intrusion prevention technology and continuously updated antivirus technology). The percentage seen in **Table 10** below represents the lowest percentage implementation for each agency's top three performing metrics. The right-hand column captures the total number of agency metrics that met the 90% threshold. As seen in **Table 10**, nine of the 24 CFO Act agencies achieved this threshold. The gray cells in the table indicate agencies that did not meet this target.

Table 10: Malware Defense FY 2015

Agency	Malware Defenses FY 2015 (%)	Number of Metrics Meeting CAP Goal
HUD	100	4
OPM	100	4
State	99	4
Justice	100	3
DOT	100	3
SSA	100	3
Labor	99	3
Treasury	94	3
GSA	94	3
Interior	88	2
NRC	85	2
USAID	53	2
VA	50	2
NASA	10	2
DOD	81	1
SBA	68	1
DHS	62	1
NSF	62	1
Commerce	52	1
ED	37	1
USDA	81	0
HHS	81	0
Energy	55	0
EPA	62	0
CFO Act Agency Average	76	2

Source: Analysis of FISMA Data-Agency Level Questions (Questions 4.3, 4.4, 4.8, 4.11, 6.1.4) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

In addition to the metrics that clearly fell under either Anti-Phishing Defense or Malware Defense, there were a number of other metrics related to this CAP priority area. These metrics were collected under the "Other Defenses" heading. For this initiative, agencies were required to achieve 90% on two of the four of metrics (e.g., % of privileged user accounts that have a technical control preventing internet access and % of outbound traffic checked at the boundary for data exfiltration). As seen in **Table 11**, 19 of the 24 CFO Act agencies achieved this threshold. The gray cells in the table indicate performance that fell below the 100% target.

Table 11: Other Defenses FY 2015

Agency	Other Defenses FY 2015 (%)	Number of Metrics Meeting CAP Goal
HUD	100	4
Treasury	100	4
State	100	3
OPM	100	3
SSA	100	3
USAID	100	3
USDA	100	2
Commerce	100	2
DOD	100	2
HHS	100	2
Interior	100	2
DOT	100	2
VA	100	2
GSA	100	2
NRC	100	2
NSF	100	2
SBA	100	2
DHS	97	2
Labor	94	2
Justice	63	1
ED	67	0
Energy	34	0
NASA	17	0
EPA	0	0
CFO Act Agency Average	86	2

Source: Analysis of FISMA Data-Agency Level Questions (Questions 4.1, 4.10, 4.12, and 4.14) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

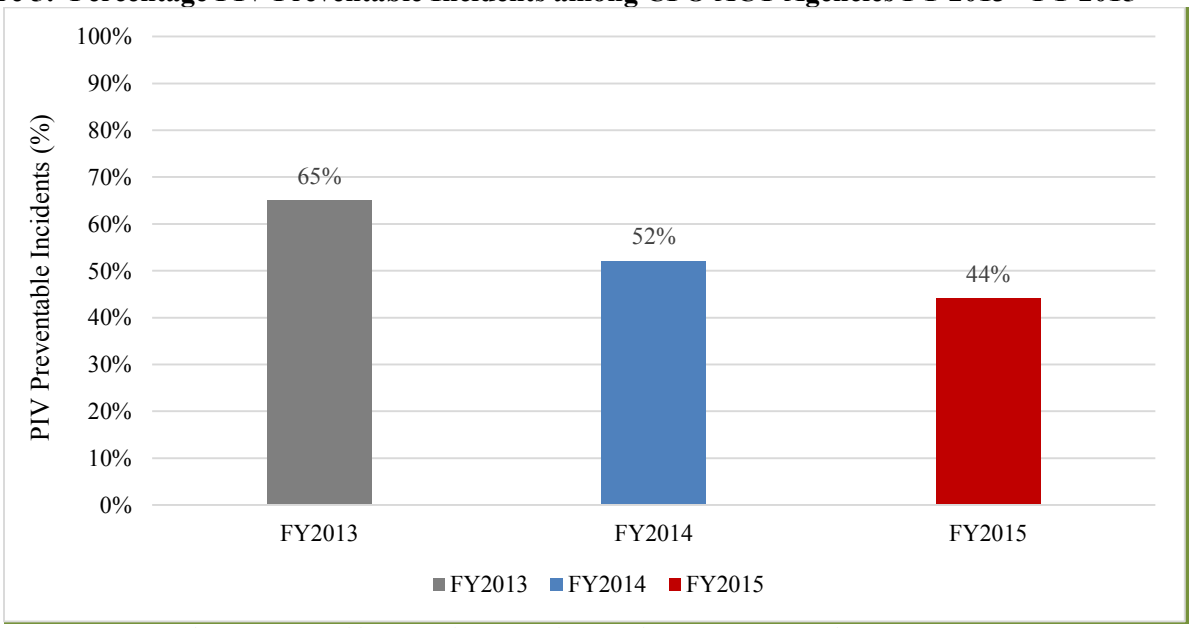
C. OMB STRONG AUTHENTICATION ANALYSIS

The *FY 2014 FISMA Report* included an assessment of the cybersecurity incidents reported to US-CERT and assessed the information to determine how many were related to or could have been prevented by the use of PIV cards. Given the high number of incidents that fell into this category, Strong Authentication remained a CAP goal and was central to efforts to bolster Federal cybersecurity during the Cybersecurity Sprint. OMB's analysis separates information security incidents into four categories:

1. Improper Usage, Policy Violation, Suspicious Network Activity, and Unauthorized Access – Improper user behavior can be deterred by reducing anonymity through Strong Authentication.
2. Social Engineering, Phishing, and Malicious Code – These incident types can be deterred through use of PIV card capabilities such as digitally signing emails and delivering corresponding user training to prevent phishing attempts.
3. Denial of Service, Equipment, and Other – These incident types are not typically related to Strong Authentication implementation.
4. Non-Cyber – OMB removed this incident type from analysis as it does not include cybersecurity incidents.

Based on these incident groupings, OMB found that 44% of Federal civilian cybersecurity incidents in FY 2015 potentially could have been prevented by PIV implementation. As seen in **Figure 5**, there has been a consistent decline in the percentage of incidents that were related to or could have been prevented by PIV implementation since FY 2013.

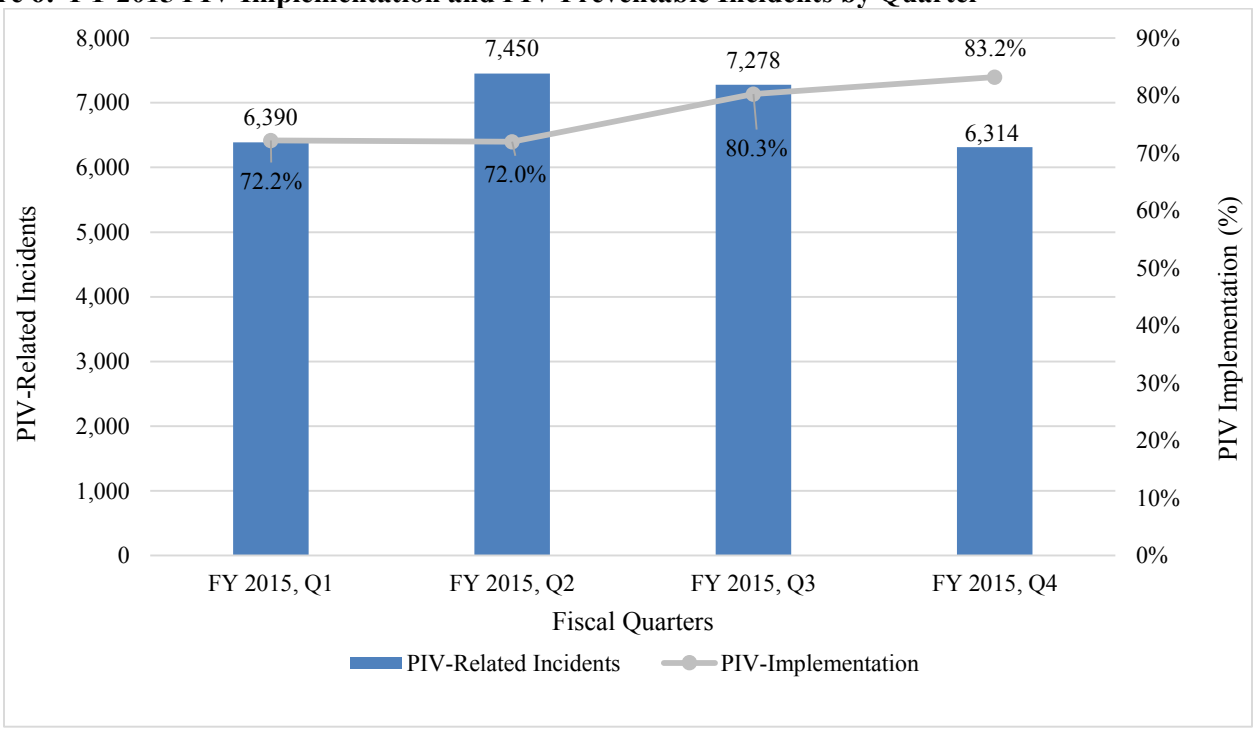
Figure 5: Percentage PIV Preventable Incidents among CFO ACT Agencies FY 2013 - FY 2015



Source: Data reported to US-CERT Incident Reporting System from October 1, 2013, to September 30, 2015.

Despite the decrease, incidents potentially prevented by PIV still make up a significant portion of Federal cybersecurity incidents. However, as PIV implementation increased between the second and fourth quarters of FY 2015, these incidents decreased by approximately 16%. **Figure 6** shows the correlation between the increase in PIV implementation throughout FY 2015 and the decrease in incidents that were related to or could have been prevented by PIV during this period.

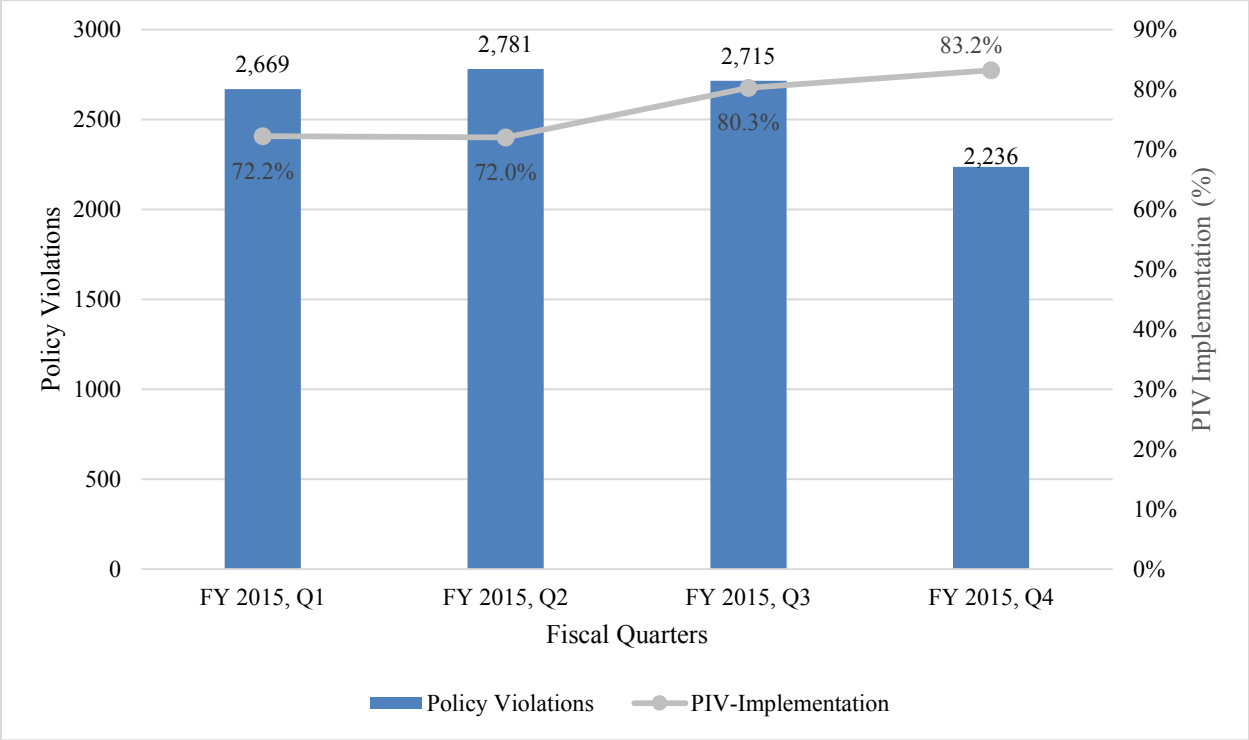
Figure 6: FY 2015 PIV Implementation and PIV Preventable Incidents by Quarter



Source: Data reported to US-CERT Incident Reporting System from October 1, 2013, to September 30, 2015.

Additionally, CFO Act agencies saw a dramatic decrease in the number of policy violations due to increased PIV implementation. Policy violations are a category of incidents characterized by the mishandling of data in storage or transit, such as digital PII records or procurement sensitive information found unsecured, or users emailing PII without proper encryption. Policy violations are the most widely PII-related cybersecurity incident reported to US-CERT. PIV implementation increases accountability and reduces anonymity, which are essential to combatting insider threats and other policy violations. **Figure 7** shows the correlation between the increase in PIV implementation throughout FY 2015 and the decrease in policy violations during this period.

Figure 7: FY 2015 PIV Implementation and Policy Violations by Quarter



Source: Data reported to US-CERT Incident Reporting System from October 1, 2013, to September 30, 2015.

While such progress is encouraging, the Federal average is still below the targets, and work remains to increase agency performance across all three Strong Authentication categories. OMB will continue to provide guidance to agencies and help identify resources to ensure agencies can achieve these targets.

SECTION III: SUMMARY OF INSPECTORS GENERAL FINDINGS

FISMA Section 3555 requires each agency's IG to perform an independent evaluation of their department's information security programs and practices. Many IGs conduct annual FISMA audits in accordance with *Generally Accepted Government Auditing Standards* or inspections pursuant to the *Quality Standards for Inspection and Evaluation* in order to assess their agencies' cybersecurity programs. Each agency's IG was asked to assess his or her department's information security programs in ten areas and upload their information into CyberScope. These ten areas were:

- ISCM;
- Configuration management;
- Identity and access management;
- Incident response and reporting;
- Risk management;
- Security training;
- Plans of action and milestones (POA&M);
- Remote access management;
- Contingency planning; and
- Contractor systems

In FY 2015, IGs instituted a new maturity model, developed in conjunction with OMB and DHS, to better assess the effectiveness of agency progress implementing ISCM capabilities. This model examines four attributes to place an agency's ISCM program in one of five maturity levels (starting with the lowest):

1. Ad Hoc
2. Defined
3. Consistently Implemented
4. Managed and Measurable
5. Optimized

For the remaining nine cybersecurity areas, all IGs' assessments include an analysis that consists of two parts:

1. Determining if a program was in place for the nine cybersecurity areas;[5] and,
2. Evaluating a combined 83 attributes of those programs.[6]

The results of these analyses were uploaded into DHS's CyberScope and used to develop this summary. **Table 12** lists the cybersecurity areas and number the metrics or attributes IGs used to perform their assessments.

Table 12: Attributes by Cybersecurity Area

No.	Cybersecurity Program Area	Attributes
1	ISCM	4
2	Configuration management	11
3	Identity and access management	8
4	Incident response and reporting	7
5	Risk management	15
6	Security training	6
7	POA&M	8
8	Remote access management	11
9	Contingency planning	11
10	Contractor systems	6
	Total	**87**

It is important to note that the IG assessment is separate from the annual assessments conducted by OMB and DHS. The two assessments are based on differing methodologies, where the IGs assess the existence of information security program components, and OMB and DHS use the FISMA metrics for CIOs to assess program quality and the degree of implementation.

Additionally, and consistent with FISMA requirements, OMB and DHS continue to work with members of the Council of the Inspectors General on Integrity and Efficiency Information Technology Committee (CIGIE) to determine possible methods for validating agency performance reported through the FISMA metrics process. To this end, OMB and DHS are working with the CIGIE to assess the extent to which they can better align the CIO FISMA metrics with the IG FISMA metrics. OMB, DHS and CIGIE envision that this work, coupled with the Inspectors General maturity model for continuous monitoring and ongoing oversight, will help provide consistent and comparable assessments of agencies' cybersecurity performance. The following section summarizes IG results for (1) CFO Act agencies and (2) small agencies; additional information on the IGs' independent assessments are available in **Appendix 4**.

CFO Act Agencies

As shown in **Table 13**, most agencies (21 of 24) have a maturity level of two or less in continuous monitoring, which would not be considered effective.

Table 13. Status of ISCM Programs by Maturity Level (CFO Act Agencies)

Maturity Level	No. of Agencies	%
Ad Hoc	15	63%
Defined	6	25%
Consistently Implemented	2	8%
Managed and Measurable	0	0%
Optimized	0	0%
Not Scored	1	4%

As shown in **Table 14**, the majority of CFO Act agencies have programs in each of the remaining nine cybersecurity areas. Twenty or more agencies have programs in place for remote access. Programs not in place were more prevalent in the areas of configuration management, identity and access management, and risk management, with up to fifteen agencies not having one or more of these programs.

Table 14: Status of CFO Act Agency Programs by Cybersecurity Area, except for ISCM

Cyber Security Program Area[a]	Program in place		Program not in place	
	No.	%	No.	%
Configuration management	16	70%	7	30%
Identity and access management	17	74%	6	26%
Incident response and reporting	19	83%	4	17%
Risk management	13	57%	10	43%
Security training	19	83%	4	17%
POA&M	18	78%	5	22%
Remote access management	21	91%	2	9%
Contingency planning	18	78%	5	22%
Contractor systems	16	70%	7	30%

Source: Data provided to DHS via CyberScope from November 14, 2014, to November 13, 2015.

[a] Due to the size of the Department, the DOD IG did not provide a definitive yes or no response; therefore, only 23 agencies are included in these areas.

Table 15 provides the CFO Act agencies' cybersecurity assessment scores for fiscal years 2015, 2014, 2013, and 2012. For ISCM, the score was prorated based on the level of maturity and was calculated using the new scoring methodology. The remaining areas were scored based on (1) whether or not a program was in place for each area, and (2) how many attributes were found in each agency's cybersecurity program. The table is ordered by FY 2015 scores. One agency scored over 90% (green), which is a decrease of five from FY 2014. Thirteen agencies scored between 65% and 90% (yellow), and the remaining nine scored lower than 65% (red). The average score for reporting agencies was 68% for FY 2015—a decrease of 8% from last year. The new scoring methodology, which reflects the effectiveness oriented maturity model scoring for ISCM, has contributed to this decline in scores.

Table 15: CFO Act Agencies' Scores

Agency	FY 2015 (%)	FY 2014 (%)	FY 2013 (%)	FY 2012 (%)
GSA	91	99	98	99
Justice	89	99	98	94
DHS	86	98	99	99
NRC	86	96	98	99
NASA	85	95	91	92
SSA	84	96	96	98
NSF	81	87	88	90
Labor	79	82	76	82
EPA	77	84	77	77
VA	75	80	81	81
Energy	75	78	75	72
USAID	73	86	83	66
ED	73	91	89	79
OPM	69	74	83	77
Treasury	58	67	76	76
HHS	58	35	43	50
Interior	57	92	79	92
Commerce	55	N/A†	87	61
SBA	51	58	55	57
DOT	48	63	61	53
USDA	43	53	37	34
HUD	39	19	29	66
State	34	42	51	53
DOD	N/A*	N/A*	N/A*	N/A*

Source: Data provided to DHS via CyberScope from November 14, 2014, to November 13, 2015.
* Due to the size of the Department, the DOD IG is unable to definitively report a yes or no answer for all FISMA attributes.
† Commerce IG's FISMA audit scope was reduced as a result of (1) attrition of several key IT security staff, (2) the need to complete audit work assessing the security posture of key weather satellite systems that support a national critical mission, and (3) additional office priorities. As a result, the FISMA submission primarily focused on assessing policies and procedures, and covered a limited number of systems that would not warrant computation of a compliance score.

For FY 2015, we also assessed the CFO Act agencies' results by type of attribute or metric. DHS designated each attribute or metric as an administrative priority (AP), a key FISMA metric (KFM) or a base metric. **Table 16** compares each agency's overall score with its compliance with (1) APs and (2) APs combined with KFMs. Agencies that scored over 90% are green, agencies that scored between 65% and 90% are yellow, and those that scored lower than 65% are red. This provides an indication as to how well agencies have addressed the priority and key metrics as compared to their performance over all metrics combined. For purposes of ISCM, the AP metric was considered to be accomplished if the agency had a maturity level of two or more.

Table 16: CFO Act Agencies' Scores (All Attributes, APs, and KFMs) for FY 2015

Agency	FY 2015		
	All Attributes (%)	Administrative Priorities (AP) (%)	AP Plus Key FISMA Metrics (%)
GSA	91	100	92
Justice	89	67	82
DHS	86	100	91
NRC	86	100	100
NASA	85	67	91
SSA	84	100	91
NSF	81	100	100
Labor	79	67	82
EPA	77	67	91
VA	75	100	73
Energy	75	33	82
USAID	73	0	64
ED	73	67	73
OPM	69	67	82
Treasury	58	0	55
HHS	58	100	64
Interior	57	67	73
Commerce	55	0	55
SBA	51	0	36
DOT	48	0	18
USDA	43	67	55
HUD	39	67	55
State	34	67	45

Source: Data provided to DHS via CyberScope from November 15, 2012, to November 14, 2014.
*Due to the size of the Department, the DOD IG is unable to definitively report a yes or no answer for all FISMA attributes.

Small Agencies

The results for the small agencies that reported were comparable to those of the 24 CFO Act agencies. **Table 17** summarizes the maturity level results for these agencies in the ISCM area.

Table 17. Status of ISCM Programs by Maturity Level (Small Agencies)

Maturity Level	No. of Agencies	%
Ad Hoc	25	53%
Defined	16	34%
Consistently Implemented	22	44%
Managed and Measurable	1	2%
Optimized	0	0%
Not Scored	33	66%

Table 18 summarizes the results from the IGs of the small agencies for the remaining cyber security areas. These results indicate that the small agencies performed best (i.e., had programs in place) in identity and access management, security training, and remote access management. The weakest performances (i.e., highest number of cases where programs were not in place) occurred in configuration management, risk management, contingency planning, and contractor systems. Some agencies that did report did not necessarily address all programs. Hence, the table will not reflect the same total number of agencies in all program areas.

Table 18: Results for Small Agencies by Cyber Security Area

Cyber Security Program Area*	Program in place		Program not in place	
	No.	%**	No.	%**
Configuration management	24	56%	19	44%
Identity and access management	30	70%	13	30%
Incident response and reporting	34	79%	9	21%
Risk management	24	56%	19	44%
Security training	34	79%	9	21%
POA&M	30	70%	13	30%
Remote access management	32	76%	10	24%
Contingency planning	31	72%	12	28%
Contractor systems	27	68%	13	32%

Source: Data provided to DHS via CyberScope from November 14, 2014, to November 13, 2015.
* One or more IGs did not report a program in place.
** Percent rounded.

Table 19 provides the small agencies' compliance scores for FY 2015, FY 2014, and FY 2013. The table is organized according to agencies' FY 2015 compliance scores. These agencies were scored using the same method applied to the CFO Act agencies, including the new scoring methodology used for ISCM. Five agencies scored over 90% (green), 21 scored between 65% and 90% compliance (yellow), and 13 scored less than 65% (red). The remaining seven small agencies did not provide data. The average score was 69% for FY 2015, which is comparable to the CFO Act agencies. The new scoring methodology, which reflects the effectiveness oriented maturity model scoring for ISCM, has contributed to this decline in scores.

Table 19: Small Agencies' Compliance Scores

Agency	FY 2015 (%)	FY 2014 (%)	FY 2013 (%)
Selective Service System	98	100	N/A
Inter-American Foundation	95	N/A	N/A
National Transportation Safety Board	93	100	78
Federal Energy Regulatory Commission	93	100	99
Commodity Futures Trading Commission	91	95	81
Chemical Safety Board	89	N/A	N/A
Federal Housing Finance Agency	86	95	95
Federal Trade Commission	86	91	92
National Credit Union Administration	86	95	83
Armed Forces Retirement Home	86	56	N/A
National Endowment for the Humanities	84	90	87
Board of Governors of the Federal Reserve System	84	87	88
Export-Import Bank of the United States	82	98	96
International Boundary and Water Commission	81	72	53
Merit Systems Protection Board	80	83	88
National Endowment for the Arts	80	98	N/A
Overseas Private Investment Corporation	79	98	84
Federal Maritime Commission	79	66	54
Equal Employment Opportunity Commission	77	95	99
Securities and Exchange Commission	77	77	80
Farm Credit Administration	76	92	99
Consumer Financial Protection Bureau	75	81	72
Smithsonian Institution	73	87	88
Federal Deposit Insurance Corporation	73	82	87
Millennium Challenge Corporation	73	94	84
Tennessee Valley Authority	68	82	99
Federal Mediation and Conciliation Service	66	65	65
International Trade Commission	66	57	51
Pension Benefit Guaranty Corporation	65	64	71
Federal Communications Commission	63	36	N/A
National Labor Relations Board	60	59	87
Railroad Retirement Board	59	73	80
Committee for Purchase from People Who Are Blind or Severely Disabled	56	N/A	N/A
Corporation for National and Community Service	55	57	72
Federal Labor Relations Authority	52	70	84

Denali Commission	47	N/A	N/A
Court Services and Offender Supervision Agency	44	39	71
National Archives and Records Administration	43	16	N/A
Peace Corps	40	48	33
Defense Nuclear Facilities Safety Board	34	47	N/A
Consumer Product Safety Commission	28	36	30
Office of Special Counsel	28	N/A	N/A
Broadcasting Board of Governors	19	47	50
Federal Election Commission	N/A	N/A	N/A
Federal Retirement Thrift Investment Board	N/A	N/A	N/A
Other Defense Civil Programs	N/A	N/A	74

Source: Data provided to DHS via CyberScope from November 14, 2014, to November 13, 2015.
NOTE: Federal Election Commission, Federal Retirement Thrift Investment Board did not provide answers with the detail required for scoring for FY 2015. Federal Election Board, and Other Defense Civil Programs did not report answers for FY 2015.

SECTION IV: PROGRESS IN MEETING KEY PRIVACY PERFORMANCE MEASURES

Protecting individual privacy remains a top Administration priority. The Federal Government increasingly uses IT to collect, maintain, and disseminate personal information. Federal agencies must take steps to analyze and address privacy risks at the earliest stages of the planning process, and must continue to manage information responsibly throughout the life cycle of the information.

Federal agencies also must continue to work closely with their SAOP to ensure compliance with all 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 completed 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 to implement appropriate data breach response procedures and update those procedures as needed.

Across the Federal Government, agencies are expected to demonstrate continued progress in all aspects of privacy protection. In FY 2015, all 24 CFO Act agencies and 46 non-CFO Act agencies reported privacy performance measures to OMB.

Table 20: CFO Act Agencies' Progress in Meeting Key Privacy Performance Measures

Key Privacy Performance Measures – CFO Act Agencies	FY 2013	FY 2014	FY 2015
Number of systems containing information in identifiable form	4,395	4,406	4,601
Number of systems requiring a PIA	2,586	2,701	2,940
Number of systems with a PIA	2,436	2,564	2,428
Percentage of systems with a PIA	**94%**	**95%**	**83%**
Number of systems requiring a SORN	3,343	3,346	3,414
Number of systems with a SORN	3,196	3,217	3,260
Percentage of systems with a SORN	**96%**	**96%**	**96%**

Source: Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2014, to September 30, 2015.

Table 21: Non-CFO Act Agencies' Progress in Meeting Key Privacy Performance Measures

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

Source: Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2014, to September 30, 2015.

Privacy Program Oversight by the Senior Agency Official for Privacy

In FY 2015, 23 out of 24 CFO Act agencies' SAOPs reported participation in all three privacy responsibility categories (including privacy compliance activities, assessments of information technology, and evaluating legislative, regulatory, and other agency policy proposals for privacy). One CFO Act agency reported SAOP participation in two out of the three categories. Of the 46 non-CFO Act agencies that reported privacy measures to OMB, 31 SAOPs reported participation in all three privacy responsibility categories, while six reported participation in two categories, two reported participation in one category, and seven reported no participation in any of the three categories.

In addition, the following percentages of CFO Act and non-CFO Act agency SAOPs provided formal written advice or guidance in each of the following categories:

Table 22: SAOP Formal Written Advice and Guidance

SAOP Provided Formal Written Advice or Guidance on:	CFO Act Agencies	Non-CFO Act Agencies
Agency policies, orders, directives, or guidance governing the agency's handling of PII	100%	90%
Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching, and similar issues	88%	70%
Agency's practices for conducting, preparing, and releasing SORNs and PIAs	100%	74%
Reviews or feedback outside of the SORN and PIA process (e.g., formal written advice in the context of budgetary or programmatic activities or planning)	96%	63%
Privacy training (either stand-alone or combined with training on related issues)	100%	91%

Source: Data reported to DHS via CyberScope and provided to OIRA from October 1, 2014, to September 30, 2015.

Mandated Policy Compliance Reviews

The Privacy Act of 1974 (5 U.S.C. § 522a.), the E-Government Act of 2002 (44 U.S.C. §101), and OMB guidance require Federal agencies to conduct certain reviews. In FY 2015, 23 out of 24 CFO Act agencies reported having current documentation demonstrating review of the agency's compliance with information privacy laws, regulations, and policies. Similarly, 23 CFO Act agencies reported having documentation demonstrating review of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified during compliance reviews. All but four CFO Act agencies reported using technologies that enable continuous auditing of compliance with their stated privacy policies and practices, and all but one reported coordinating with their respective agency's Inspector General on privacy program oversight.

Thirty-five of the 46 non-CFO Act agencies that reported privacy performance measures to OMB reported having current documentation demonstrating review of the agency's compliance with information privacy laws, regulations, and policies. Thirty-three non-CFO Act agencies reported having documentation demonstrating review of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified during compliance reviews. Thirty-six non-CFO Act agencies reported coordinating with their respective agency's Inspector General on privacy program oversight. Finally, only 20 non-CFO Act agencies reported using technologies that enable continuous auditing of compliance with their stated privacy policies and practices.

Privacy Impact Assessments

The goal for the Federal Government is for 100% of applicable systems to be covered by PIAs. In FY 2015, 83% 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 83% figure reported by CFO Act agencies represents a decrease in the compliance rate compared to previous years. In contrast, the 85% figure reported by non-CFO Act agencies represents an increase in the compliance rate compared to FY 2014. Moreover, all 24 CFO Act agencies reported having a centrally located page on the agency's website that provides working links to agency PIAs. Of the non-CFO Act agencies that reported having systems that require a PIA, 11 reported not having a centrally located page that provides working links to the agency PIAs.

In addition, the following percentages of agencies reported having written policies or processes in place for the following privacy practices:

Table 23: Formal Agency Policies and Practices for PIAs

Have Written Policies or Processes in Place for:	CFO Act Agencies	Non-CFO Act Agencies
Determining whether a PIA is needed	100%	87%
Conducting a PIA	100%	83%
Evaluating changes in technology or business practices that are identified during the PIA process	100%	78%
Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA	100%	80%
Making PIAs available to the public as required by law and OMB policy	100%	72%
Monitoring the agency's systems and practices to determine when and how PIAs should be updated	100%	74%
Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained	100%	76%

Source: Data reported to DHS via CyberScope and provided to the OIRA from October 1, 2014, to September 30, 2015.

System of Records Notices

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 2015, 96% of CFO Act agencies' and 90% of non-CFO Act agencies' systems with Privacy Act records have a published, up-to-date SORN. In addition, all CFO Act agencies reported having a centrally located page on the agency's website that provides working links to agency SORNs. Of the non-CFO Act agencies that reported having systems that require a SORN, eight reported not having a centrally located page that provides working links to published SORNs.

Privacy Training

Twenty-three of the 24 CFO Act agencies reported having a program to ensure that all personnel who handle personal information, who are directly involved in the administration of personal information or information technology systems, or that have significant information security responsibilities, receive job-specific and comprehensive information privacy training. Thirty-six of the 46 non-CFO Act agencies that reported privacy metrics to OMB reported having such a policy. Moreover, 23 CFO Act agencies reported having a policy in place to ensure that all personnel with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramifications of inappropriate access and disclosure. Forty-two non-CFO Act agencies reported having such a policy.

Website Privacy Policies

In FY 2015, the following percentages of agencies reported having written policies or processes in place for the following:

Table 24: Formal Agency Web Policies and Practices

Have Written Policies or Processes in Place for:	CFO Act Agencies	Non-CFO Act Agencies
Making appropriate updates and ensuring continued compliance with stated web privacy policies	100%	74%
Determining circumstances where the agency's web-based activities warrant additional consideration of privacy implications	100%	74%
Requiring machine-readability of public-facing organization web sites (i.e., use of P3P)	88%	72%

Source: Data reported to DHS via CyberScope and provided to the OIRA from October 1, 2014, to September 30, 2015.

SECTION V: APPENDICES

APPENDIX 1: SECURITY INCIDENTS BY CFO ACT AGENCY

The charts in this appendix illustrate the types of FY 2015 security incidents reported by each CFO Act agency to the US-CERT Incident Reporting System between October 1, 2012 and November 16, 2015. Definitions used are provided by US-CERT and are the same as those listed in Section II.

Table 25: US-CERT Incident Definitions

Category/Subcategories	Definition
Denial of Service (DoS)	This category is used for all *successful* DoS incidents, such as a flood of traffic, which renders a web server unavailable to legitimate users.
Improper Usage:	Improper Usage categorizes all incidents where a user violates acceptable computing policies or rules of behavior. These include incidents like the spillage of information from one classification level to another.
-Unauthorized Access	Unauthorized Access is when an individual gains logical or physical access without permission to a Federal agency network, system, application, data or other resource. (*Subcategory of Improper Usage Category*)
-Social Engineering	Social Engineering is used to categorize fraudulent web sites and other attempts to entice users to provide sensitive information or download malicious code. Phishing is a set of Social Engineering, which is itself a subcategory of Unauthorized Access. (*Set of Unauthorized Access Subcategory*)
-Phishing	Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques, typically via emails containing links to fraudulent websites. (*Set of Social Engineering Subcategory*)
-Equipment	Equipment is used for all incidents involving lost, stolen or confiscated equipment, including mobile devices, laptops, backup disks or removable media. (*Set of Unauthorized Access Subcategory*)
-Policy Violation	Policy Violation is primarily used to categorize incidents of mishandling data in storage or transit, such as digital PII records or procurement sensitive information found unsecured or PII being emailed without proper encryption. (*Subcategory of Improper Usage Category*)
Malicious Code	Used for all *successful* executions or installations of malicious software, which are not immediately quarantined and cleaned by preventative measures such as antivirus tools.
Non Cyber	Non Cyber is used for filing all reports of PII spillages or possible mishandling of PII, which involve hard copies or printed material as opposed to digital records.
Other	For the purpose of this report, a separate superset of multiple subcategories has been employed to accommodate several low-frequency types of incident reports, such as unconfirmed third-party notifications, failed brute force attempts, port scans, or reported incidents where the cause is unknown.
Suspicious Network Activity	This category is primarily utilized for incident reports and notifications created from EINSTEIN data analyzed by US-CERT.

Source: Definitions are provided by US-CERT and available at: *https://www.us-cert.gov/government-users/reporting-requirements*

Figure 8: Security Incidents Reported - Department of Agriculture (USDA)

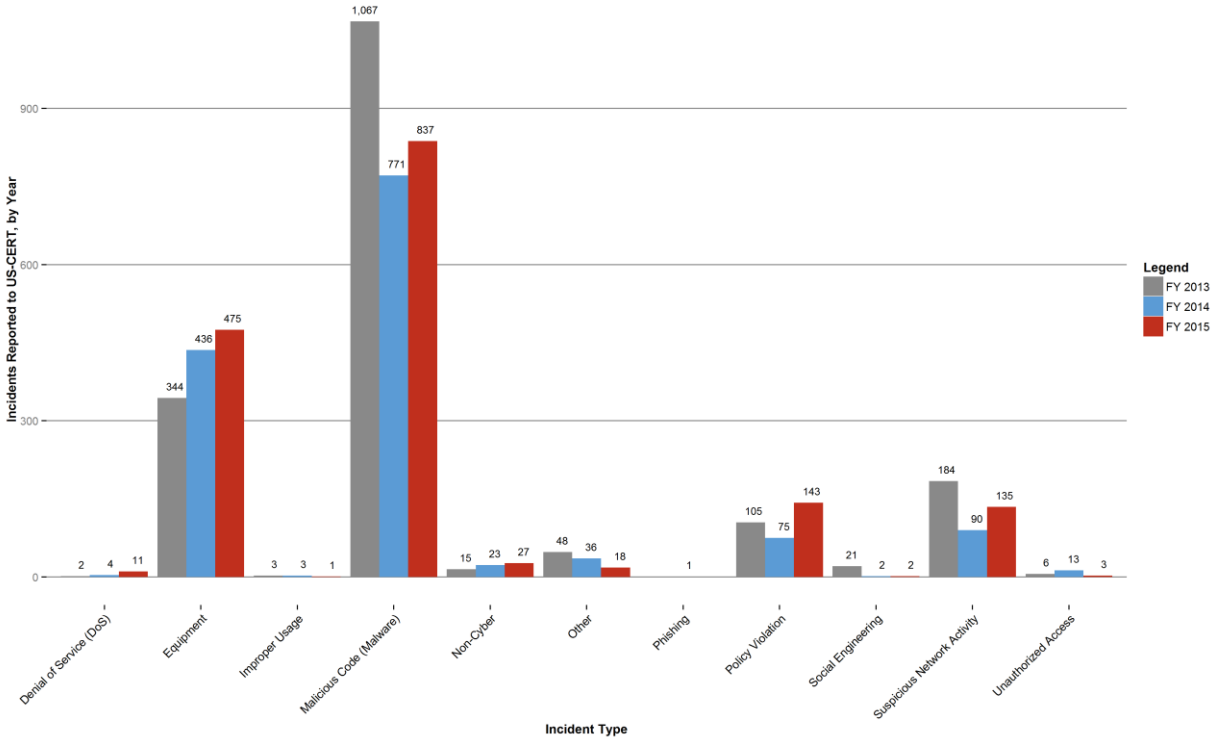


Figure 9: Security Incidents Reported - Department of Commerce (Commerce)

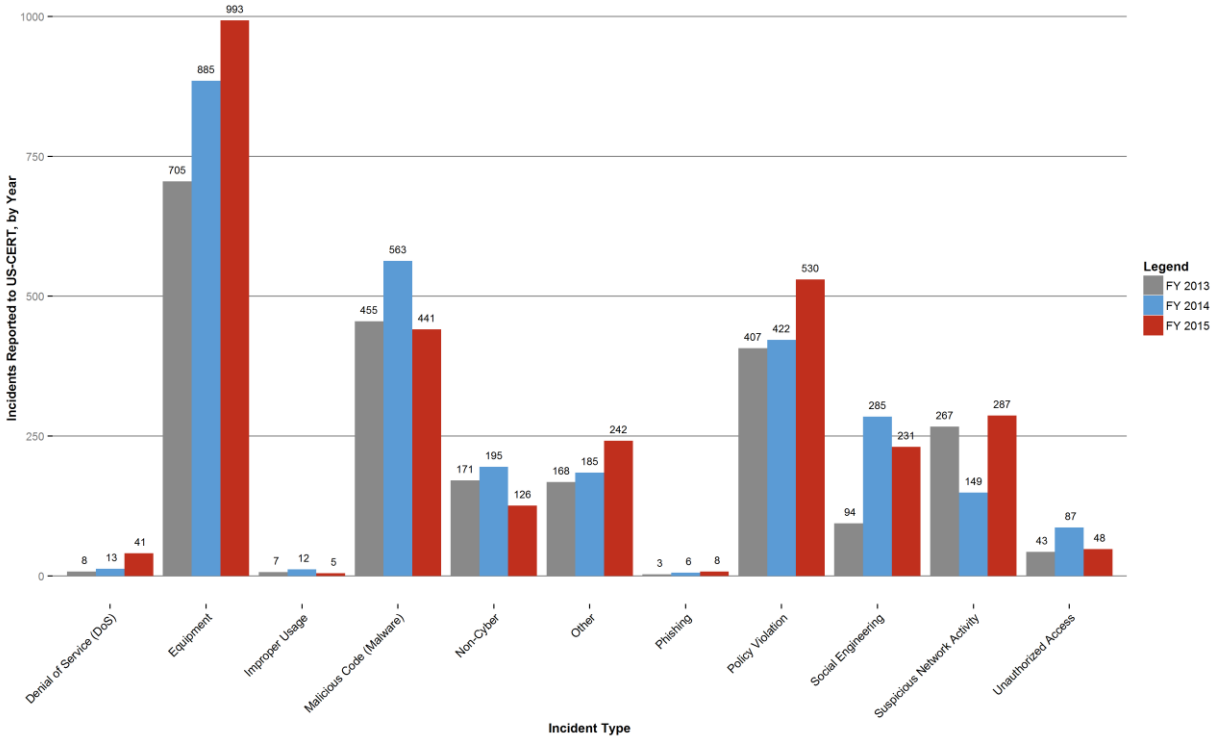


Figure 10: Security Incidents Reported - Department of Defense (DOD)

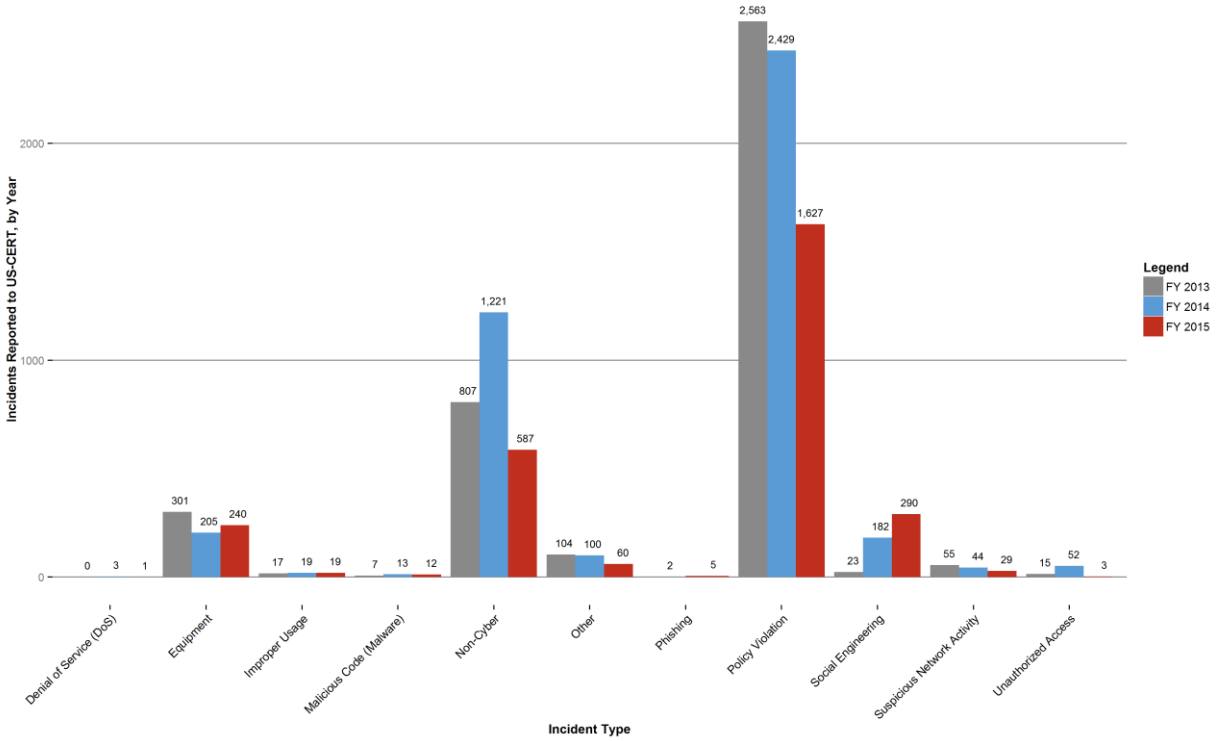


Figure 11: Security Incidents Reported - Department of Education (ED)

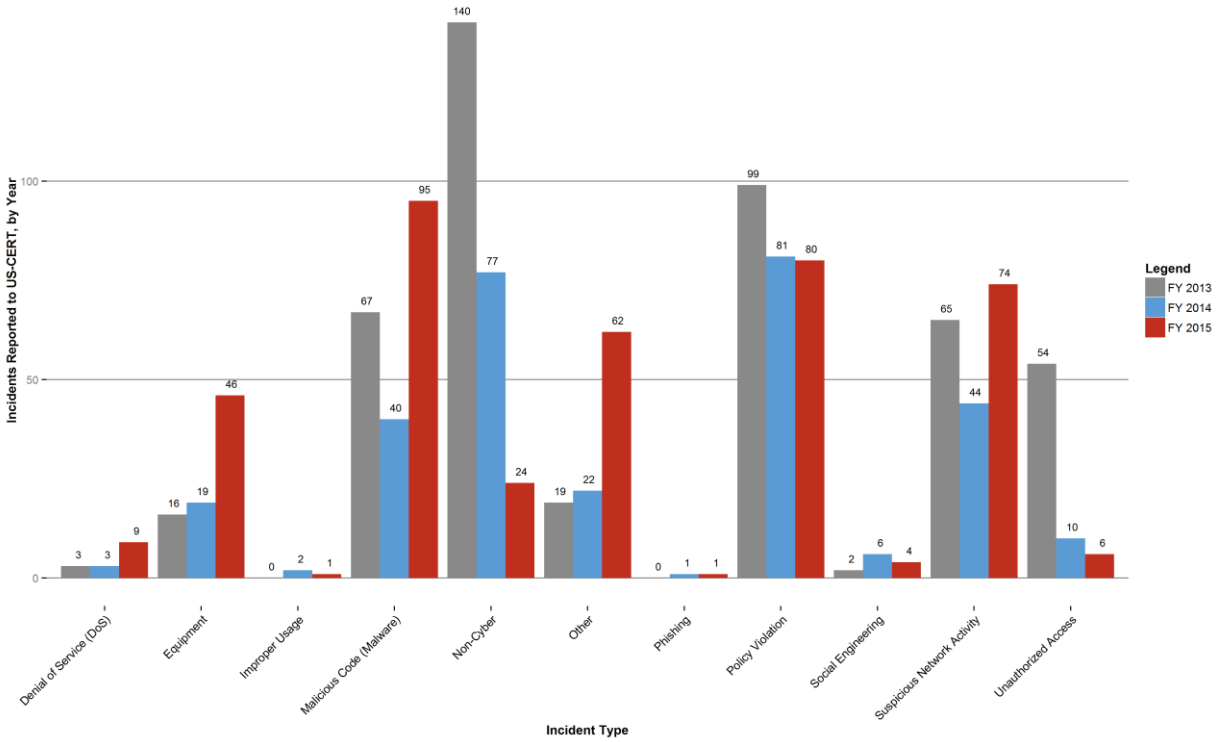


Figure 12: Security Incidents Reported - Department of Energy (Energy)

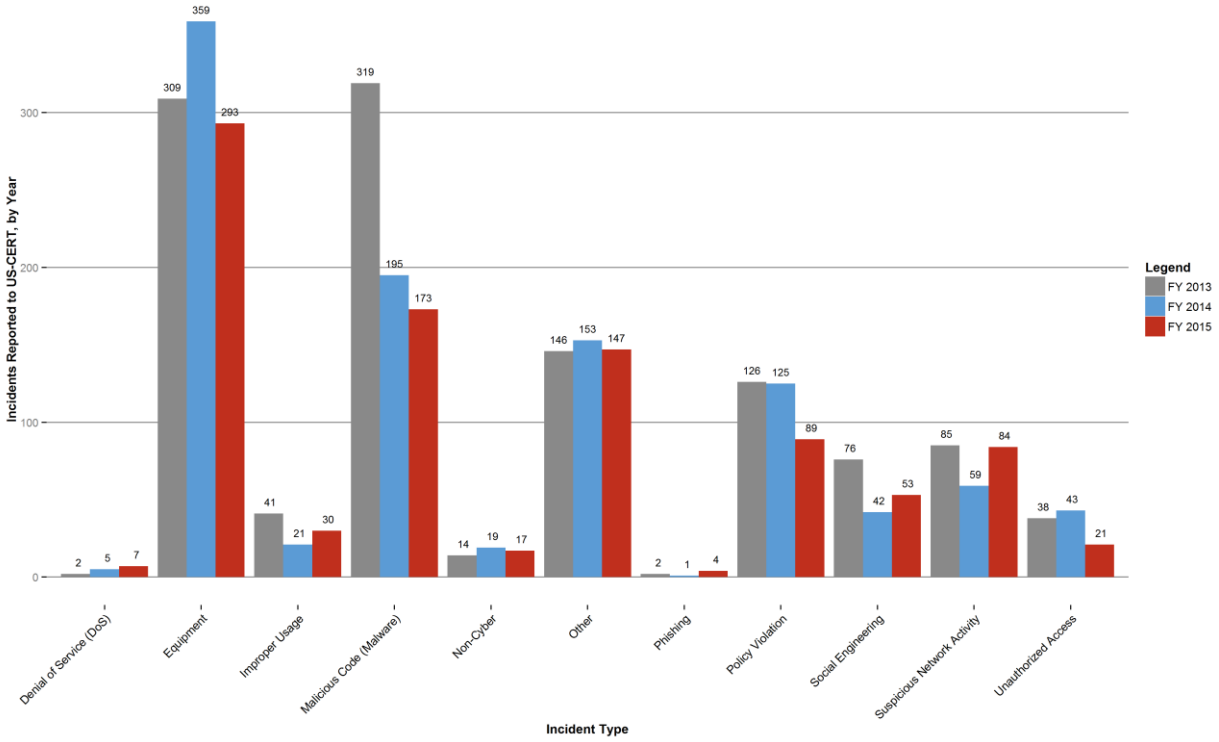


Figure 13: Security Incidents Reported - Department of Health and Human Services (HHS)

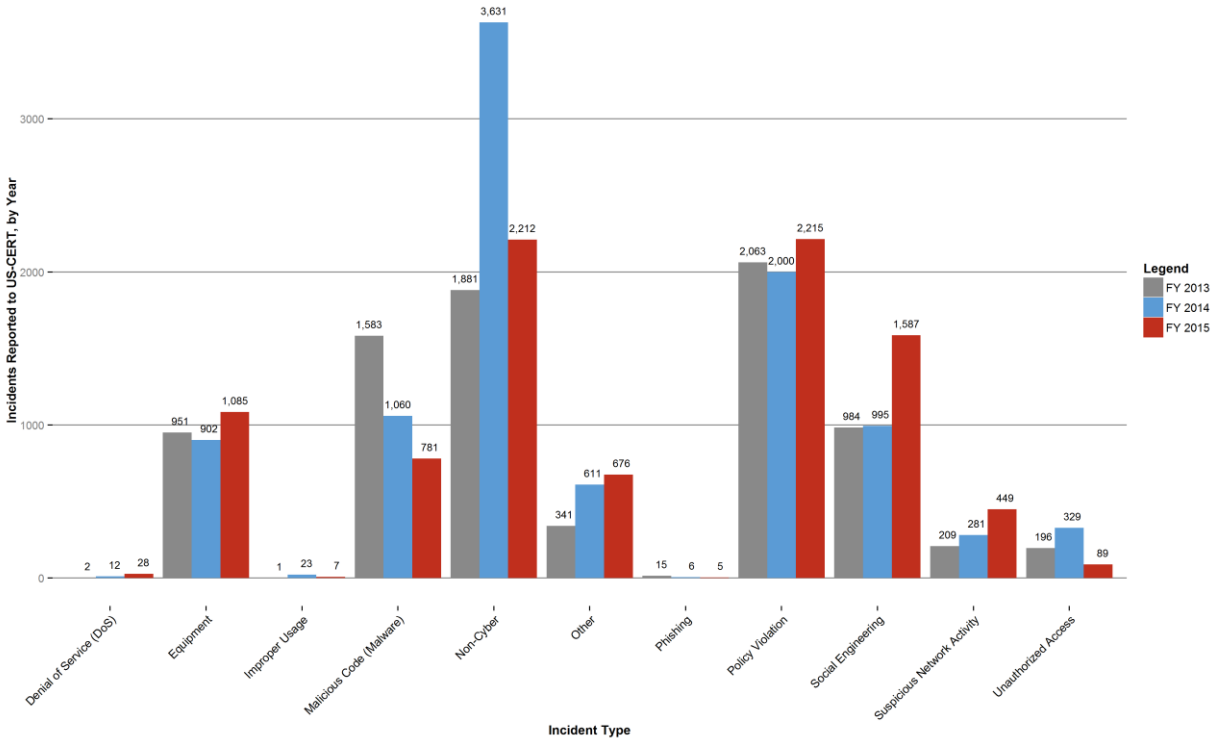


Figure 14: Security Incidents Reported - Department of Homeland Security (DHS)

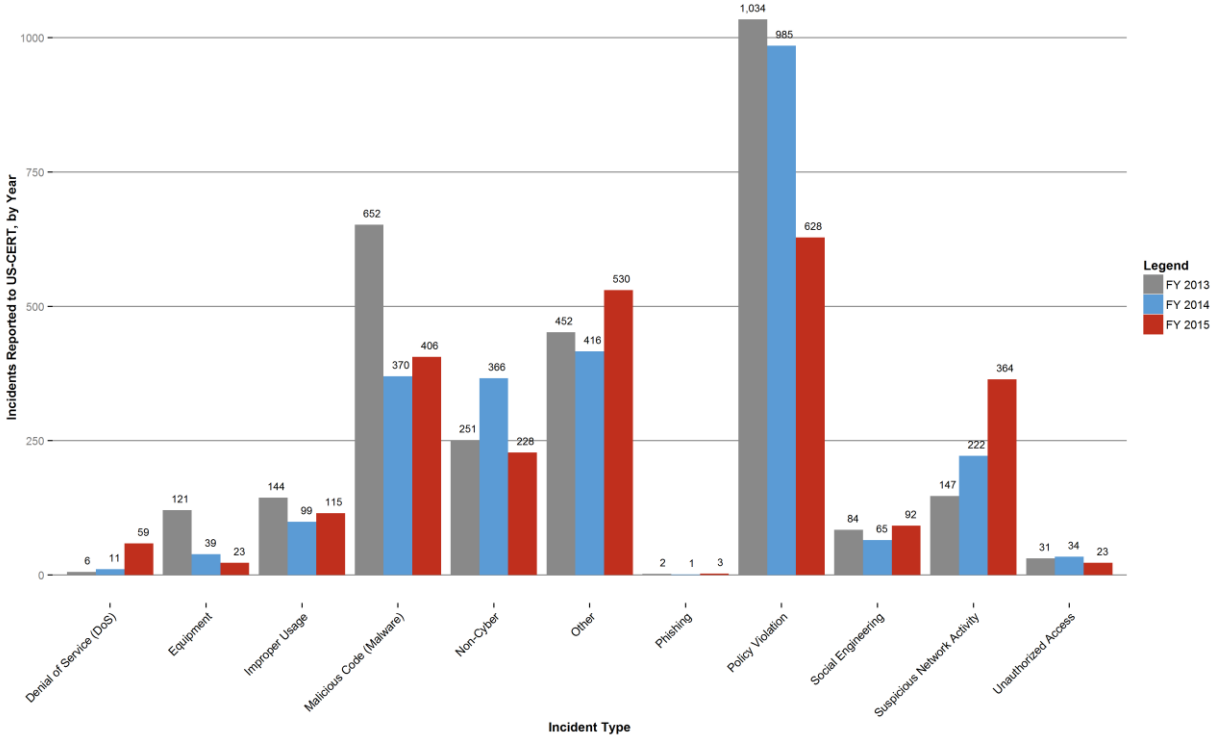


Figure 15: Security Incidents Reported - Department of Housing and Urban Development (HUD)

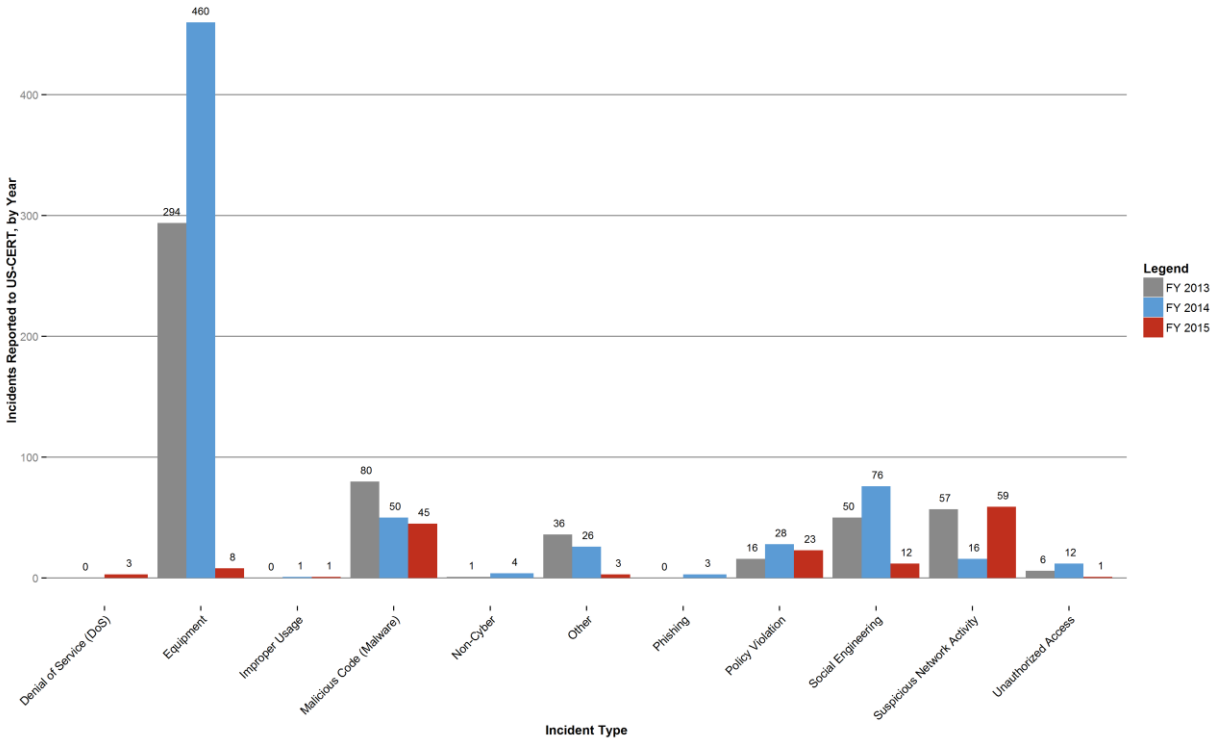


Figure 16: Security Incidents Reported - Department of the Interior (Interior)

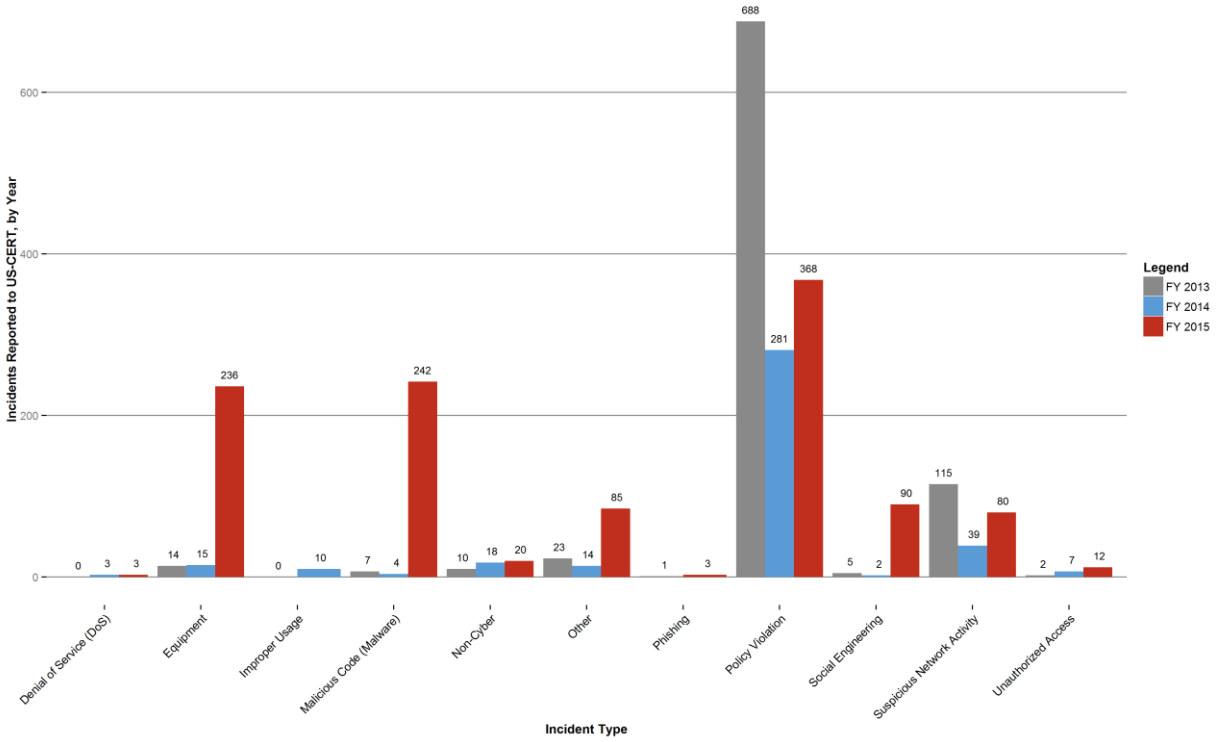


Figure 17: Security Incidents Reported - Department of Justice (Justice)

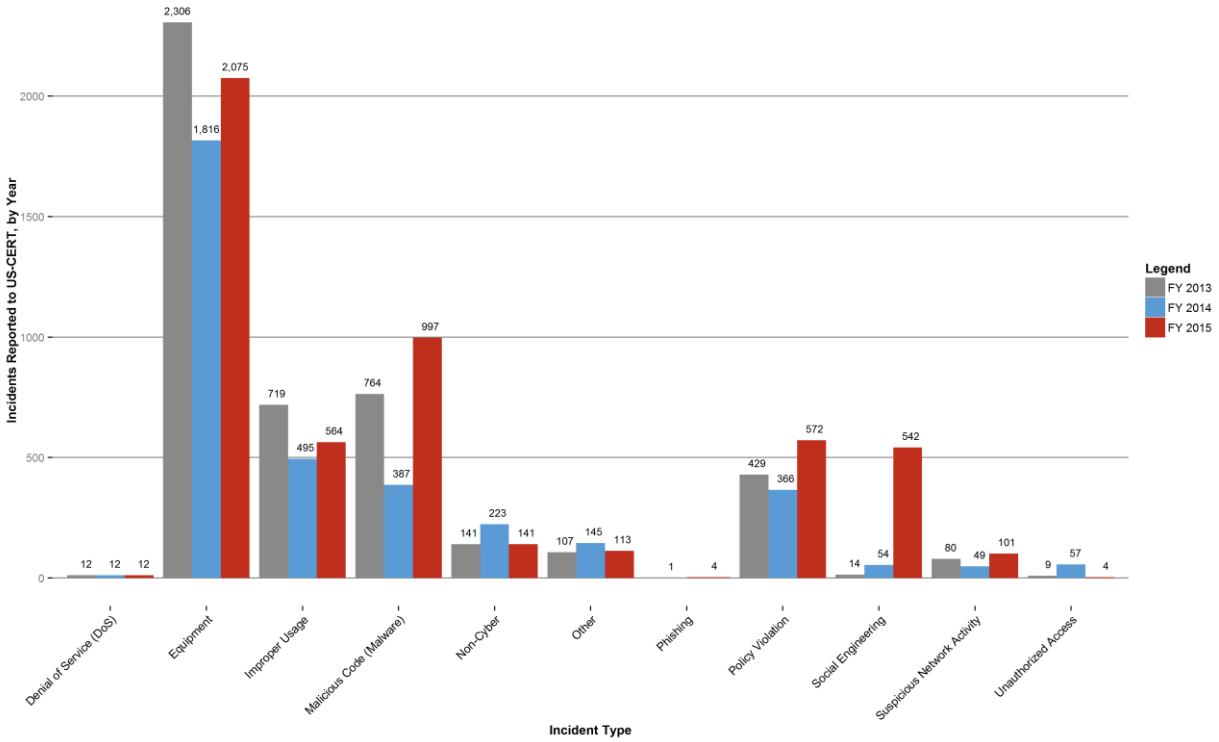


Figure 18: Security Incidents Reported - Department of Labor (Labor)

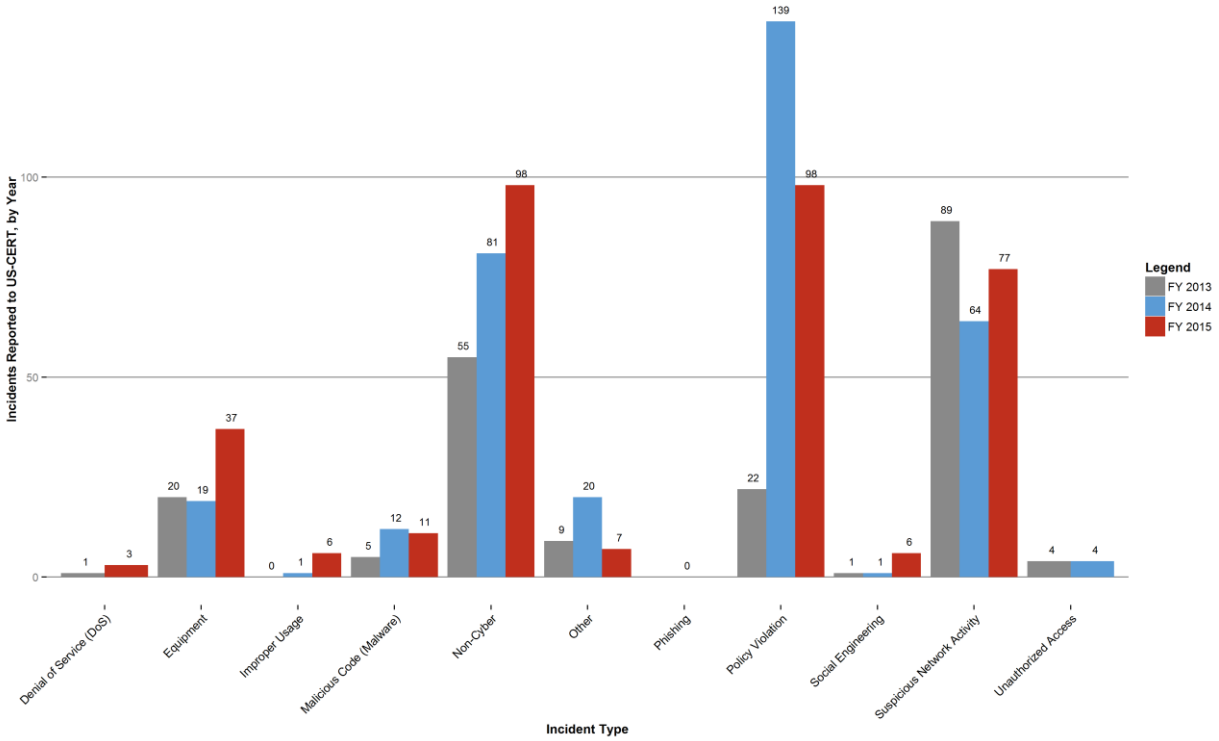


Figure 19: Security Incidents Reported - Department of State (State)

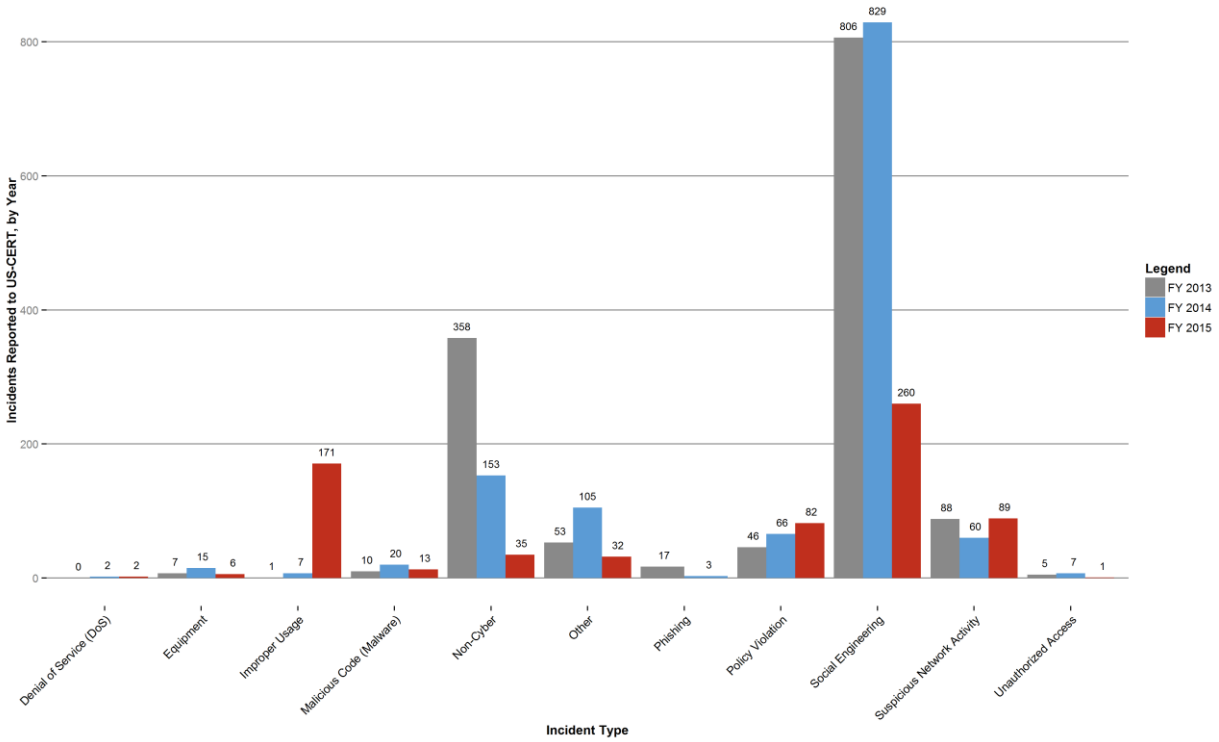


Figure 20: Security Incidents Reported - Department of the Treasury (Treasury)

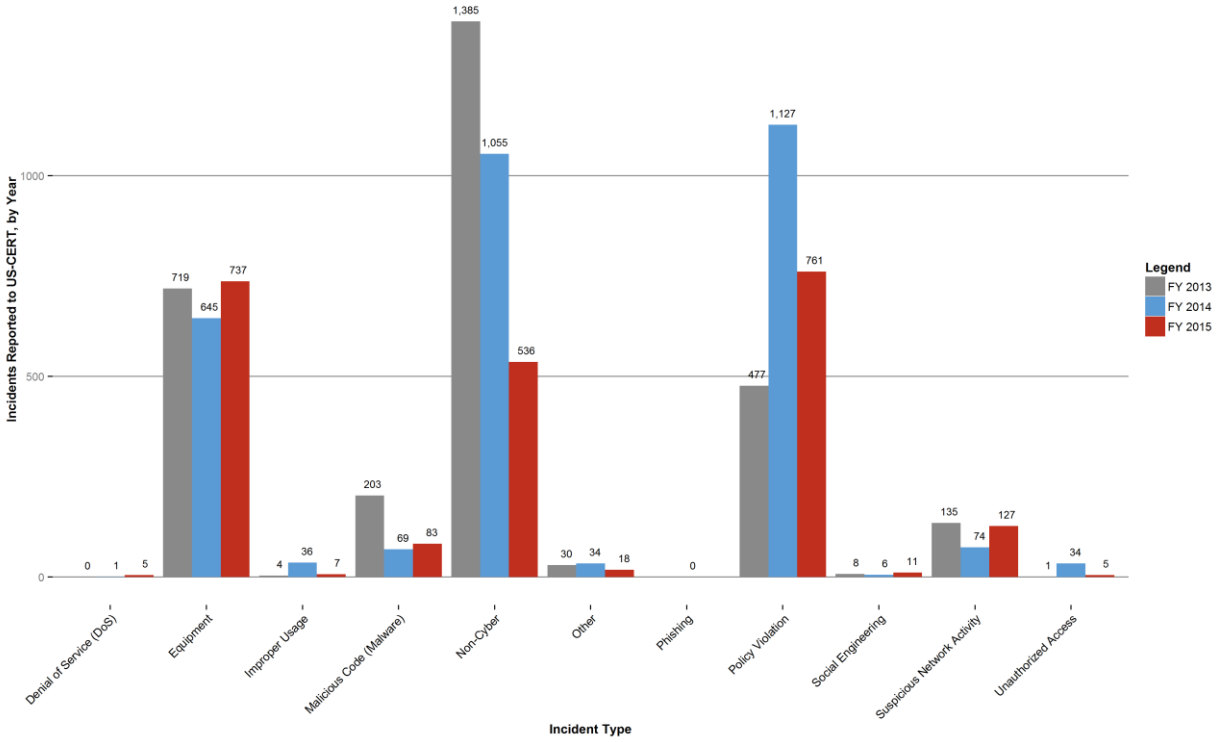


Figure 21: Security Incidents Reported - Department of Transportation (DOT)

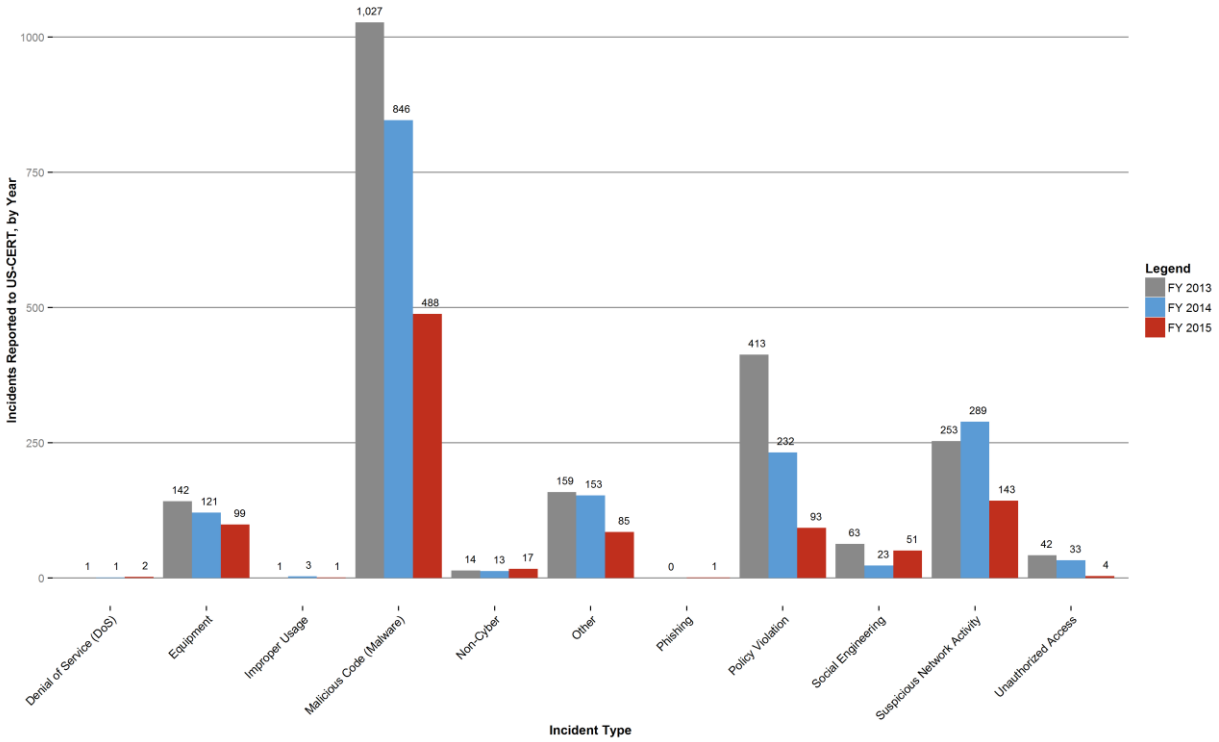


Figure 22: Security Incidents Reported - Department of Veterans Affairs (VA)

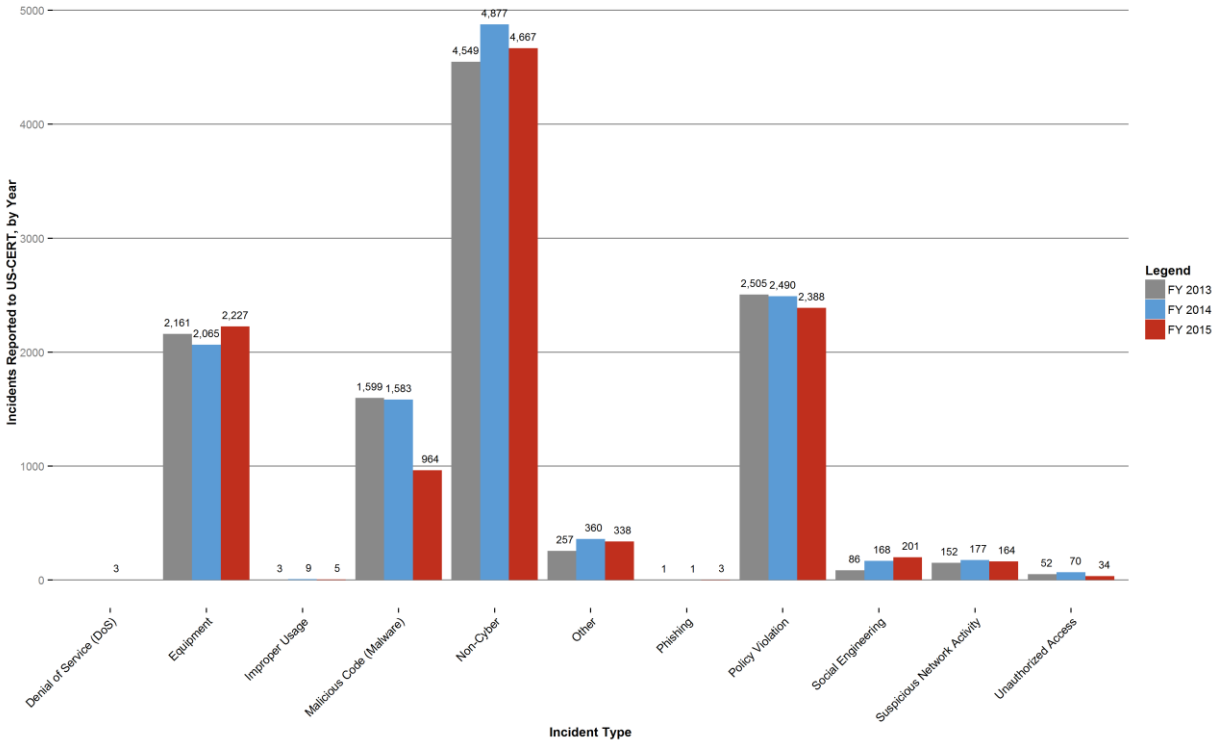


Figure 23: Security Incidents Reported - Environmental Protection Agency (EPA)

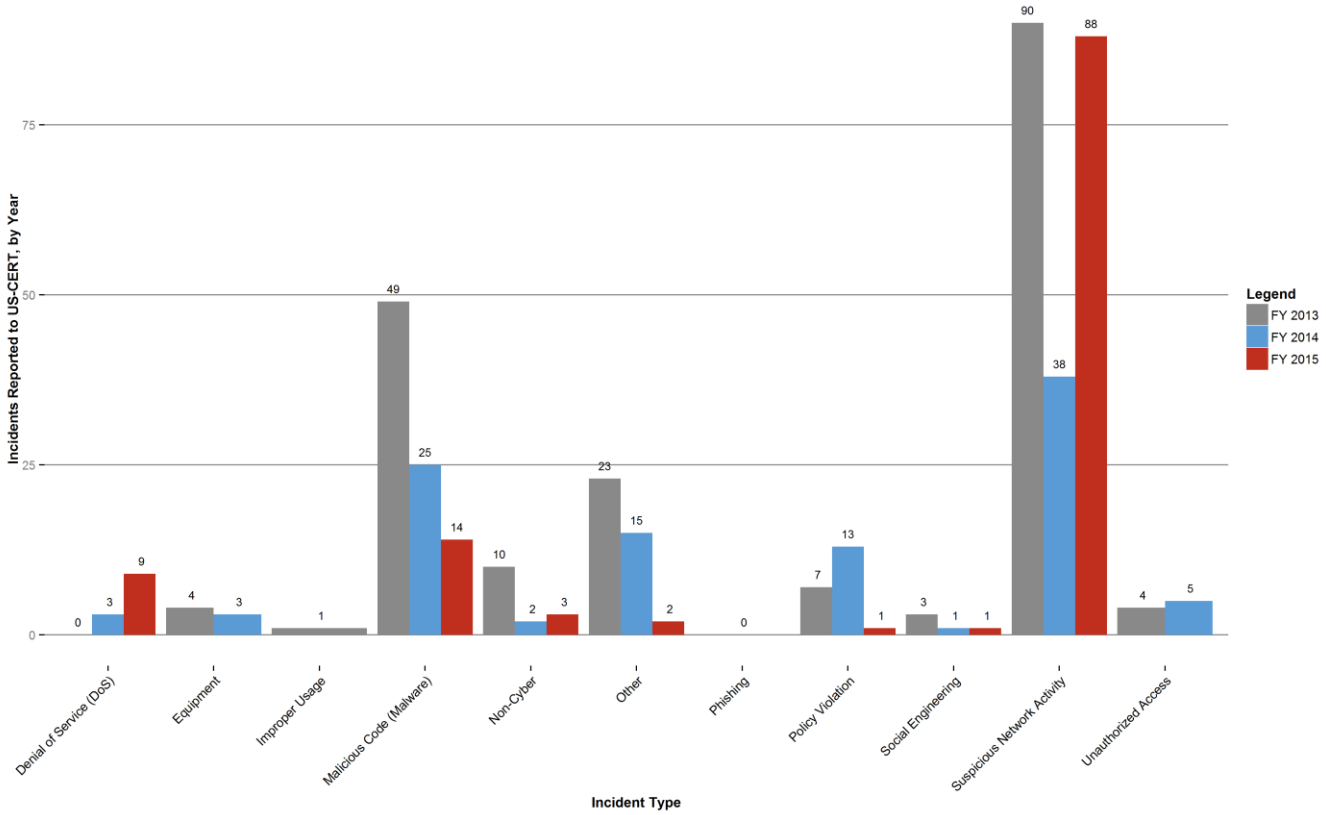


Figure 24: Security Incidents Reported - General Services Administration (GSA)

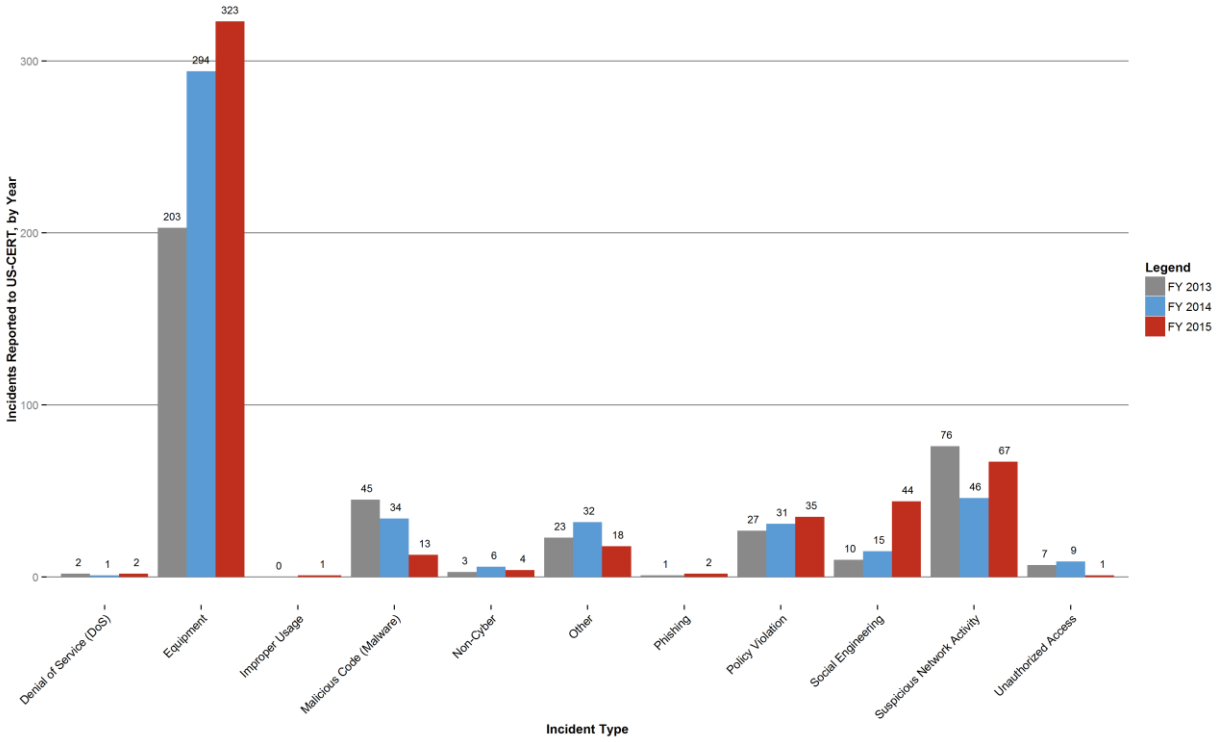


Figure 25: Security Incidents Reported - National Aeronautics and Space Administration (NASA)

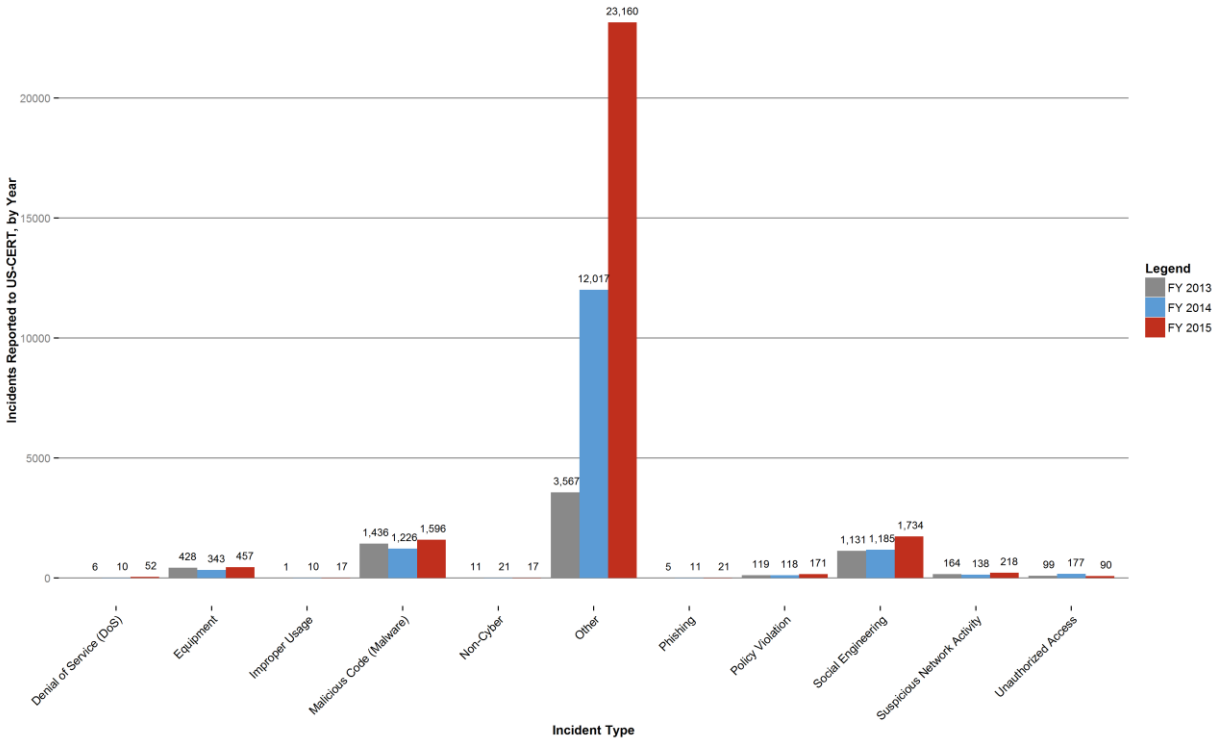


Figure 26: Security Incidents Reported - National Science Foundation (NSF)

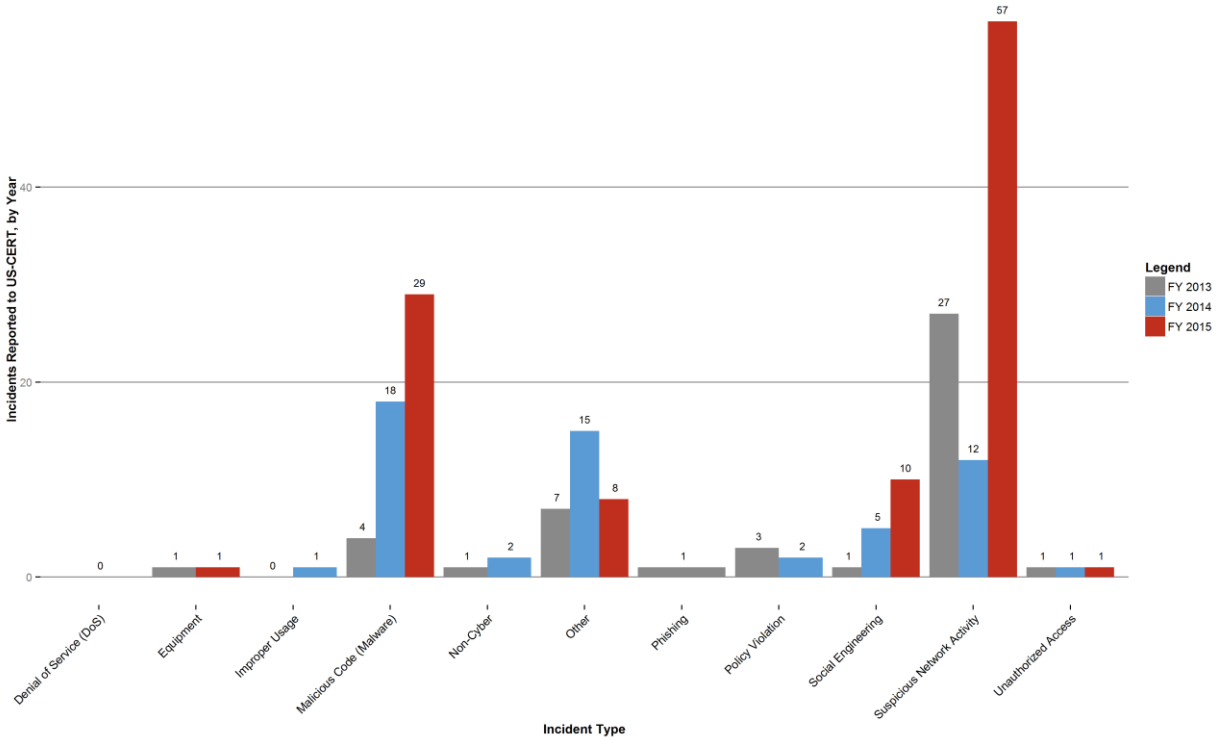


Figure 27: Security Incidents Reported - Nuclear Regulatory Commission (NRC)

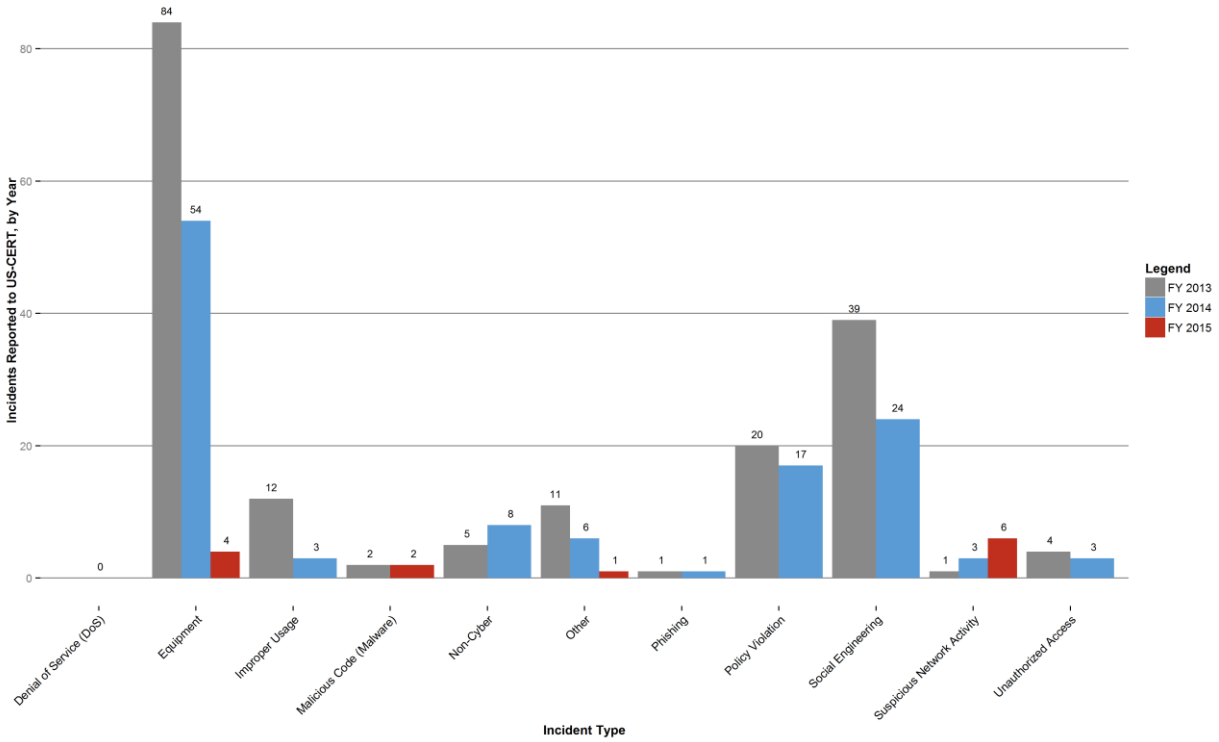


Figure 28: Security Incidents Reported - Office of Personnel Management (OPM)

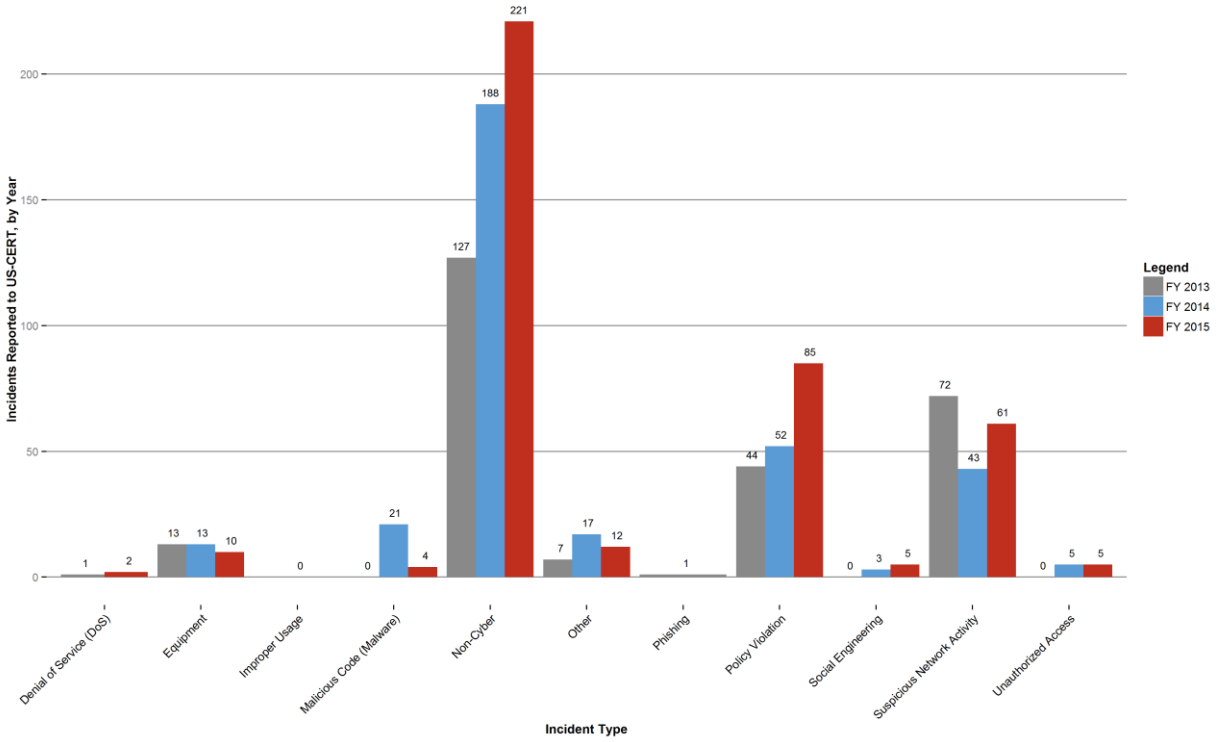


Figure 29: Security Incidents Reported - Small Business Administration (SBA)

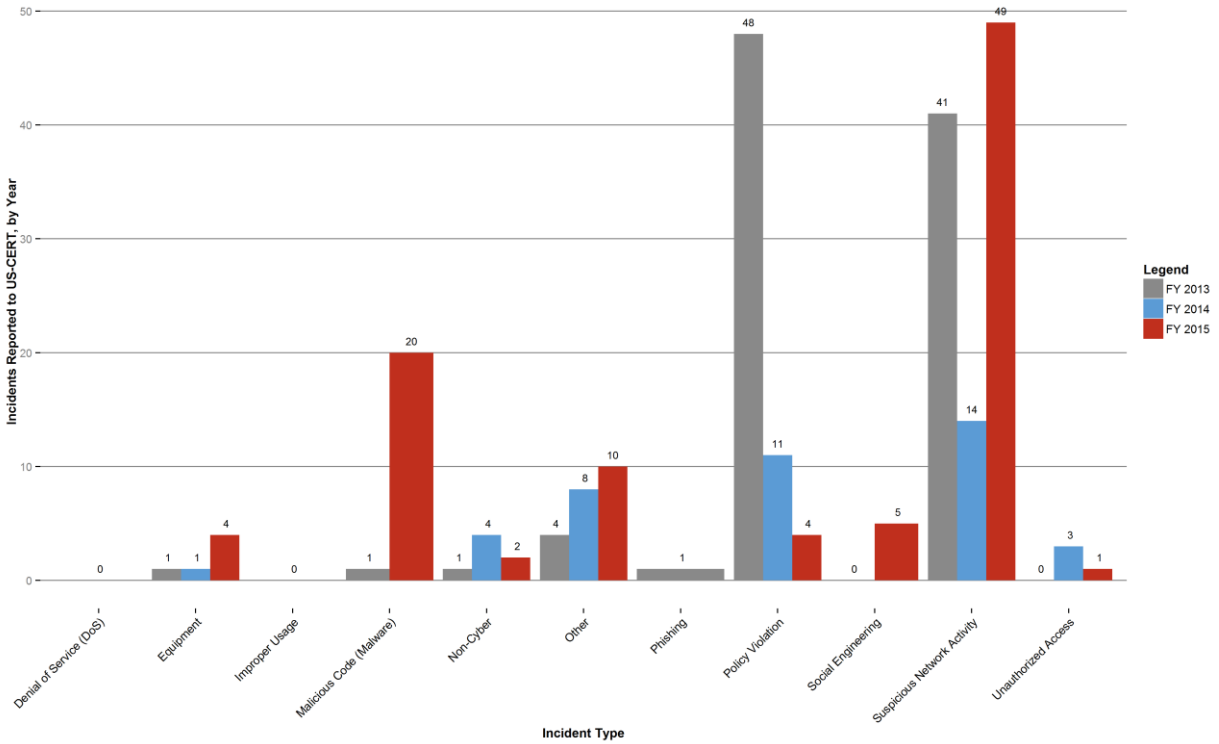


Figure 30: Security Incidents Reported - Social Security Administration (SSA)

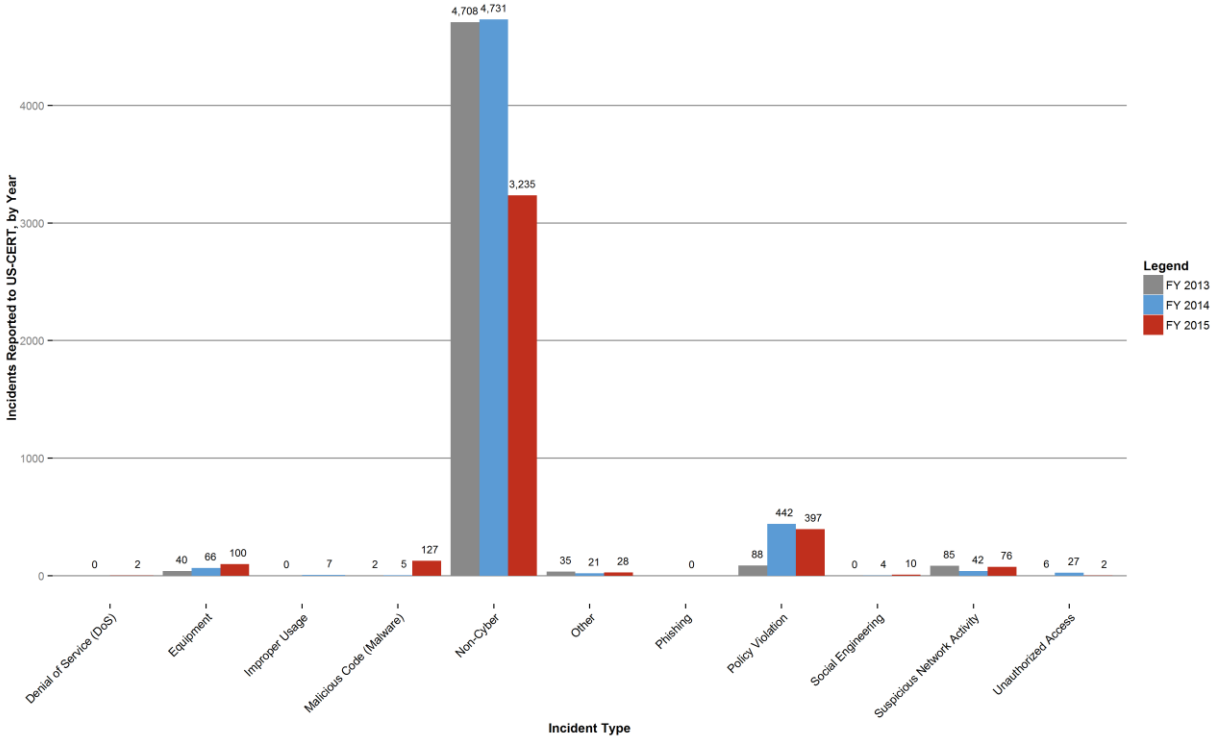
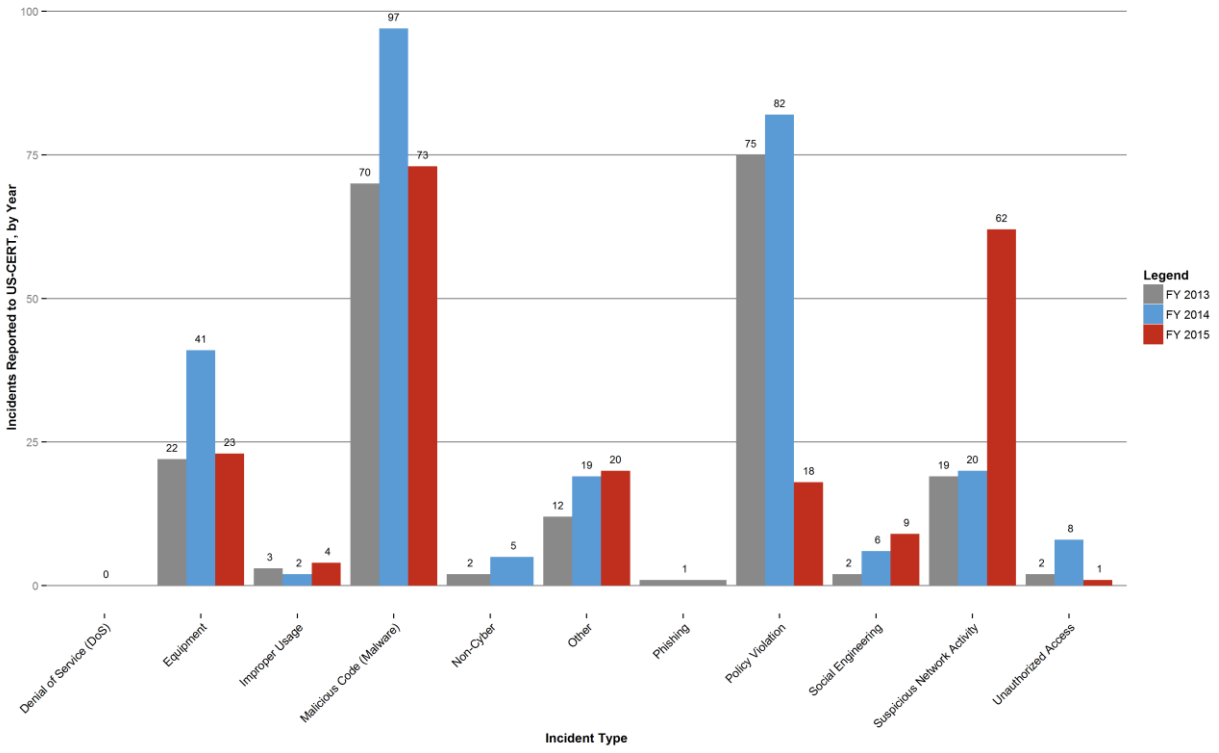


Figure 31: Security Incidents Reported - US Agency for International Development (USAID)



APPENDIX 2: CYBERSECURITY FY 2015 CAP GOAL METRICS

This Appendix identifies CAP Goal information related to the priority areas described in Section II, which represent the basic building blocks of a strong cybersecurity posture. *DHS FY 2015 CIO Annual FISMA Metrics page* contains more specific information on each metric. Additionally, in accordance with FISMA Section 3553, OMB and DHS use these metrics to assess agency compliance with NIST standards. The following sections present information into the performance of each CAP Goal metric and highlight pertinent findings to assess the state of agency cybersecurity. The following tables rank CFO Act agency performance against cybersecurity CAP goals from the highest performing to the lowest performing for each metric.

Information Security Continuous Monitoring (ISCM)

Hardware Asset Management

Agencies report on the percentage of assets covered by an automated capability to provide visibility into inventory information. Agency performance on this metric decreased from 96% in FY 2014 to 90% in FY 2015. Fifteen agencies are at or above 95%. As shown in **Table 26,** the agencies with the lowest percentage of hardware assets covered by an automated capability are EPA (64%), DOD (83%), and Commerce (85%).

Table 26: ISCM Automated Hardware Asset Management FY 2014 & FY 2015

Agency	Automated Asset Management FY 2014 (%)	Automated Asset Management FY 2015 (%)
ED	100	100
Labor	100	100
State	87	100
Treasury	99	100
DOT	96	100
GSA	100	100
NSF	100	100
NRC	89	100
OPM	95	100
SSA	100	100
SBA	100	99
USDA	99	98
DHS	99	97
Justice	99	97
USAID	85	95
HHS	93	94
VA	94	94
NASA	93	93
HUD	93	91
Interior	98	89
Energy	94	87
Commerce	86	85
DOD	97	83
EPA	76	64
CFO Act Agency Average*	96	90

*This is a weighted average based on the total number of the organization's hardware assets connected to the organization's unclassified network(s).
Source: Analysis of FISMA Agency Level Data Question 2.1 and 2.2 (FY 2014) and 2.1 and 2.3 (FY 2015), reported to DHS via CyberScope from October 1, 2013, to September 30, 2015.

CFO Act agency performance is 71% on this metric, with 10 of 24 CFO Act agencies at or above 95%. As can be seen in **Table 27**, the agencies with the lowest percentage of hardware assets covered by an automated capability are VA (0%), NASA (0%), and EPA (2%).

Table 27: ISCM Detect and Alert on Unauthorized Hardware Assets FY 2015

Agency	Assets with automated capability to detect and alert on the addition of unauthorized hardware (%)
NSF	100
NRC	100
OPM	100
SSA	100
Labor	99
DOT	99
SBA	98
Justice	97
USAID	96
USDA	95
DOD	93
HHS	92
Energy	89
Treasury	83
State	81
ED	77
GSA	73
Commerce	66
HUD	62
DHS	54
Interior	46
EPA	2
VA	0
NASA	0
CFO Act Agency Average*	72

*This is a weighted average based on the total number of the organization's hardware assets connected to the organization's unclassified network(s).
Source: Analysis of FISMA Agency Level Data (Question 2.1 and 2.2), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Software Asset Management

Agencies report on the percentage of assets covered by an automated capability to provide visibility into inventory information. **Table 28** shows CFO Act agency performance on this metric is 89%, with 17 of 24 CFO Act agencies at or above 95%. The agencies with the lowest percentage of software assets covered by an automated capability are Energy (67%), EPA (68%), and HHS (76%).

Table 28: ISCM Automated Software Asset Inventory FY 2015

Agency	Assets with automated capability to scan current state of installed software (%)
DOT	100
ED	100
HUD	100
Labor	100
NSF	100
OPM	100
SSA	100
USDA	100
Interior	99
NRC	99
GSA	98
SBA	98
State	98
Justice	97
Treasury	96
Commerce	95
USAID	95
VA	91
DHS	88
DOD	87
NASA	83
HHS	76
EPA	68
Energy	67
CFO Act Agency Average*	89

*This is a weighted average based on the total number of the organization's endpoints connected to the organization's unclassified network(s).
Source: Analysis of FISMA Agency Level Data (Questions 2.1.2 and 2.6), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

As part of the oversight of agency asset management practices, agencies report on the percentage of applicable assets for which the organization has implemented an automated capability to detect and block unauthorized software from executing, for which no software exists for the device type. As can be seen in **Table 29** below, CFO Act agency performance on this metric is 68%, with seven of 24 CFO Act agencies at or above 95%. The agencies with the no reported software asset management are HUD, VA, NSF, and USAID

Table 29: ISCM Software Asset Management Detect and Block Unauthorized Software FY 2014 & FY 2015

Agency	Assets with automated capability to detect and block software FY 2014 (%)	Assets with automated capability to detect and block software FY 2015 (%)
OPM	100	100
SSA	100	100
USDA	54	100
State	85	98
Justice	99	97
GSA	98	96
Labor	98	96
NRC	89	92
Treasury	36	91
DOT	73	90
DOD	92	82
Commerce	50	72
EPA	77	67
DHS	51	58
Interior	55	57
Energy	89	39
HHS	55	32
ED	71	17
NASA	0	2
SBA	100	2
HUD	99	0
NSF	83	0
USAID	75	0
VA	0	0
CFO Act Agency Average*	69	68

*This is a weighted average based on the total number of the organization's hardware assets (FY 2014) or endpoints (FY 2015) connected to the organization's unclassified network(s).
Source: Analysis of FISMA Agency Level Data Questions 2.1 and 2.5 (FY 2014) and 2.1.2 and 2.7 (FY 2015), reported to DHS via CyberScope from October 1, 2013, to September 30, 2015.

Anti-Phishing and Malware Defense

Agencies were required to achieve 90% for a certain number of metrics comprising each initiative in order to meet the CAP goal target. For Anti-Phishing Defense, agencies had to achieve 90% coverage on five of seven metrics. For Malware Defense, agencies had to achieve 90% coverage on three of five metrics. In addition to the metrics that clearly fell under either Anti-Phishing Defense or Malware Defense, there were a number of other metrics related to this CAP priority area. These metrics were collected under the "Other Defenses" heading, and agencies were required to achieve 90% on two of four of the metrics.

Anti-Phishing Defense

Table 30 shows CFO Act agency performance on this metric is 95%, with 21 of 24 CFO Act agencies at or above the 90% target. The agencies with the lowest percentage of reported coverage are DHS (92%), DOD (85%), and EPA (0%).

Table 30: Anti-Phishing Defense: Incoming Email Analyzed FY 2015

Agency	Email traffic on systems capable of analyzing for clickable URLs, embedded content, and attachments (%)
Commerce	100
DOT	100
ED	100
GSA	100
HHS	100
HUD	100
Interior	100
Justice	100
Labor	100
NSF	100
OPM	100
SBA	100
SSA	100
State	100
USAID	100
USDA	100
VA	100
NASA	99
NRC	99
Treasury	99
Energy	98
DHS	92
DOD	85
EPA	0
CFO Act Agency Average	95

Source: Analysis of FISMA Agency Level Questions Data (Question 4.2), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Table 31 shows CFO Act agency performance on this metric is 33%, with five of 24 CFO Act agencies at or above the 90% target. Eight agencies reported no coverage in this area.

Table 31: Anti-Phishing Defense: Email Attachments FY 2015

Agency	Email on systems with the capability to open attachments in a sandboxed environment or detonation chamber (%)
Justice	100
OPM	100
State	100
HUD	95
Labor	95
USDA	90
DHS	68
Energy	42
Treasury	35
Commerce	33
DOD	15
HHS	13
NASA	8
Interior	5
DOT	1
VA	1
ED	0
EPA	0
GSA	0
NRC	0
NSF	0
SBA	0
SSA	0
USAID	0
CFO Act Agency Average	33%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.5), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Agencies report on the percentage of agency email systems that checked sender verification when receiving messages from outside the network. **Table 32** shows that EPA, NASA, and SBA have not implemented anti-spoofing technologies for receiving messages on email systems. Both Energy and Commerce have implemented these controls on fewer than 50% of their systems.

Table 32: Anti-Phishing Defense: Email Sender Authentication FY 2015

Agency	Incoming email on systems using sender authentication protocols (%)
DOD	100
DOT	100
ED	100
GSA	100
Interior	100
Labor	100
NRC	100
NSF	100
OPM	100
SSA	100
State	100
USAID	100
USDA	100
VA	100
HUD	95
Treasury	88
Justice	71
DHS	69
HHS	63
Commerce	42
Energy	38
EPA	0
NASA	0
SBA	0
CFO Act Agency Average	78%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.6), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Reputation filters identify legitimate email and blacklist known spammers in an attempt to limit the amount of spam an agency receives through its email system. This helps protect the agency and its users from potential threats associated with spam. **Table 33** shows that agencies have this capability well installed with only Commerce (83%) below the target of 90%.

Table 33: Anti-Phishing Defense: Email Scanned Using Reputation Filter FY 2015

Agency	Email on systems that use a reputation filter to perform threat assessment of sender (%)
DOD	100
DOT	100
ED	100
EPA	100
GSA	100
HHS	100
Interior	100
Justice	100
Labor	100
NASA	100
NRC	100
NSF	100
OPM	100
SBA	100
SSA	100
State	100
Treasury	100
USAID	100
USDA	100
VA	100
DHS	97
HUD	95
Energy	94
Commerce	83
CFO Act Agency Average	99%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.7), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Gateway defenses are the first line of defense in protecting agency networks. While enterprise level solutions are necessary to block/filter the majority of phishing attempts, including web content filtering, mail filtering, and mail verification. **Table 34** shows that email filtering systems are in place as part of the perimeter defenses for all the CFO Act agencies.

Table 34: Anti-Phishing Defense: Anti-Phishing/Anti-Spam Filtration FY 2015

Agency	Incoming email passing through systems with anti-phishing/anti-spam filtration technologies at the outermost border (%)
Commerce	100
DOD	100
DOT	100
ED	100
EPA	100
GSA	100
HHS	100
HUD	100
Interior	100
Justice	100
Labor	100
NASA	100
NRC	100
NSF	100
OPM	100
SBA	100
SSA	100
State	100
USAID	100
USDA	100
VA	100
Energy	99
Treasury	99
DHS	97
CFO Act Agency Average	100%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.9), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Digitally signing emails provides a degree of user authentication protecting the message recipient, who can be confident in the sender's identity. **Table 35** shows that 11 of 24 CFO Act agencies have not implemented any sender verification and anti-spoofing technologies for sending messages on their email systems. Six of 24 agencies have the capability to digitally sign outgoing email on all (100%) of their systems.

Table 35: Anti-Phishing Defense: Email Digitally Signed FY 2015

Agency	Percent (%) of sent email is digitally signed
EPA	100
GSA	100
HHS	100
Interior	100
SSA	100
VA	100
Treasury	70
Justice	64
Commerce	42
DOT	20
DHS	5
USDA	5
State	3
DOD	0
ED	0
Energy	0
HUD	0
Labor	0
NASA	0
NRC	0
NSF	0
OPM	0
SBA	0
USAID	0
CFO Act Agency Average	34%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.13), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

The most effective attempts on cyber-networks seek to exploit user behavior. Phishing attempts seek to convince users to provide information or grant access for an adversary to steal information or compromise a network. It is important for users to understand, identify, and be able to protect themselves from phishing attempts. Training privileged and unprivileged users remains a necessary deterrent to preventing phishing attempts. **Table 36** shows the percentage of network users to have successfully completed agency sponsored cybersecurity exercises focused on phishing. State (1%) and OPM (30%) had less than half their users pass these exercises, while DOD, Interior, and Justice did not conduct any cybersecurity-focused exercises.

Table 36: Anti-Phishing Defense: Users Successfully Completing Anti-Phishing Exercises FY 2015

Agency	Users that participated and successfully completed exercises focused on phishing (%)
DOT	100
ED	100
EPA	100
GSA	100
HUD	100
Labor	100
SBA	100
SSA	100
Treasury	100
USDA	100
VA	100
USAID	96
HHS	93
DHS	90
NSF	90
NASA	84
Energy	71
NRC	57
Commerce	53
OPM	30
State	1
DOD	0
Interior	0
Justice	0
CFO Act Agency Average*	91%

*This is a weighted average based on the total number of the organization's users participating in and successfully completing cybersecurity-focused exercises.
Source: Analysis of FISMA Agency Level Questions Data (Question 8.2.1), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Other Defense

Other Defense is a blend of anti-phishing and malware defenses that implement technologies to prevent, detect, and block anti-phishing attempts and malware incursion. Agencies were required to achieve 90% on two of four of the metrics. **Tables 37 through 40** show the results of four additional anti-phishing and malware defense metrics agencies must report. Prohibiting privileged accounts from accessing the Internet reduces the risk that malicious websites will utilize the elevated privileges to spread malware throughout the network. Privileged users should use unprivileged accounts to perform non-administrative tasks such as surfing the Internet. **Table 40** shows the implementation of a technical solution falls along the lines of the haves and have-nots. While five agencies have a 100% capability, ten agencies report that they do not have technical controls preventing Internet access to privileged users.

Table 37: Other Defense: Prevent Privileged User Internet Access FY 2015

Agency	Privileged user accounts that have a technical control preventing Internet access (%)
DOT	100
HUD	100
OPM	100
SBA	100
State	100
Treasury	97
ED	67
DOD	45
DHS	32
HHS	31
Labor	20
Commerce	16
Energy	12
USDA	5
EPA	0
GSA	0
Interior	0
Justice	0
NASA	0
NRC	0
NSF	0
SSA	0
USAID	0
VA	0
CFO Act Agency Average	34%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.1), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Content filtering programs screen email and web pages to make objectionable content unavailable to the user. Agencies can configure web content filters to incorporate rules to block access to websites and webpages that are likely to contain undesirable content or web-based threats against the network. **Table 38** shows that 16 of 24 agencies have implemented this capability in all (100%) email systems. Meanwhile, EPA, SBA, NASA, and Energy use a web content filter for less than 20% of their inbound network traffic.

Table 38: Other Defense: Web Content Filtering FY 2015

Agency	Inbound network traffic passing through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (%)
DOD	100
DOT	100
GSA	100
HHS	100
HUD	100
Interior	100
Labor	100
NRC	100
NSF	100
OPM	100
SSA	100
State	100
Treasury	100
USAID	100
USDA	100
VA	100
DHS	97
Commerce	83
Justice	63
ED	58
Energy	18
NASA	17
EPA	0
SBA	0
CFO Act Agency Average	81%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.10), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

By checking traffic at external boundaries for covert exfiltration of information, agencies can identify areas of compromise in real time and stop the exfiltration limiting the damage caused by an incident. **Table 39** shows 13 of 24 CFO Act agencies check all outbound communications for evidence of exfiltration. The following agencies do not have any exfiltration detection in place at their external boundaries: EPA, GSA, and NSF.

Table 39: Other Defense: Detect Covert Exfiltration of Information FY 2015

Agency	Outbound communications traffic checked at external boundaries to detect covert exfiltration of information (%)
Commerce	100
DOD	100
HUD	100
Interior	100
NRC	100
OPM	100
SBA	100
SSA	100
State	100
Treasury	100
USAID	100
USDA	100
VA	100
DHS	97
DOT	80
HHS	75
ED	69
Justice	63
Energy	34
Labor	17
NASA	8
EPA	0
GSA	0
NSF	0
CFO Act Agency Average	73%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.12), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Quarantined or blocked messages protect individual user machines and the system at large from the consequences of opening email messages infected with viruses or other nefarious programming. **Table 40** shows that eight of 24 agencies have implemented the capability to quarantine or otherwise block suspicious email on all email systems. DHS and SBA have this capability on 11% or less of their systems, while EPA and DOD respectively report 1% or no capability to quarantine or block email.

Table 40: Other Defense: Email Traffic Quarantined or Otherwise Blocked FY 2015

Agency	Percent (%) of email traffic quarantined or otherwise blocked
USAID	100
NSF	100
Commerce	100
GSA	100
SSA	100
HHS	100
HUD	100
Justice	100
Labor	94
Treasury	92
NRC	89
DOT	85
State	70
Energy	66
VA	65
ED	47
OPM	27
Interior	20
NASA	19
USDA	17
SBA	11
DHS	10
EPA	1
DOD	0
CFO Act Agency Average	63%

Source: Analysis of FISMA Agency Level Questions Data (Question 4.14), reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.

Information Security Metrics for Non-CFO Act Agencies

The non-CFO Act agencies consist of small and independent agencies managing a variety of Federal programs. Their responsibilities include issues relating to commerce and trade, energy and science, transportation, national security, and finance and culture. Approximately half of the non-CFO Act agencies perform regulatory or enforcement roles in the Executive Branch. The remaining agencies are comprised largely of grant-making, advisory, and uniquely chartered organizations. Together these agencies employ more than 100,000 Federal workers and manage billions of taxpayer dollars.

In FY 2015, 60 non-CFO Act agencies submitted FISMA reports compared to 41 small agencies in FY 2014. **Table 41** below is an aggregated summary of reported performance measures for agencies that submitted reports. Small agencies responded to the exact same set of FISMA metrics in CyberScope as the CFO Act agencies.

Table 41: CAP Goals, Definitions, Sources, and Non-CFO Act Agency Performance FY 2015

Key performance area	Sub-performance area	Definition	Source	Non-CFO Act Agency Performance Average
Information Security Continuous Monitoring (ISCM)	Hardware Asset Management CAP Goal	The lower of the two implementation percentages for the automated asset discovery capability and the capability to detect and alert on the addition of unauthorized hardware to the network.	FISMA Agency Level Questions Data (Questions 2.2, and 2.3) reported to DHS via CyberScope from October 1, 2014 to September 30, 2015.	50%
	Software Asset Management CAP Goal	The lower of the two implemtation percentages for the automated software asset inventory capability and the capability to detect and block unauthorized software from executing.	FISMA Agency Level Questions Data (Questions 2.6 and 2.7) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.	22%
	Secure Configuration Management CAP Goal	Percentage of the applicable hardware assets of each kind of operating system software that has an automated capability to identify deviations from the approved configuration baselines and provide visibility at the organization's enterprise level.	FISMA Agency Level Secure Configuration Management Assets and Percentage Data (Question 2.10.1 and 2.10.6) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.	80%

Key performance area	Sub-performance area	Definition	Source	Non-CFO Act Agency Performance Average
	Vulnerability Management CAP Goal	Percentage of hardware assets that are assessed using credentialed scans with Security Content Automation Protocol validated vulnerability tools.	FISMA Agency Level Questions Data (Question 2.11) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015.	65%
ICAM / Strong Authentication	Unprivileged Users CAP Goal	Percentage of unprivileged users that are required to log on to the network with a two-factor Personal Identity Verification (PIV) card or NIST Level of Assurance 4 credential.	FISMA Agency Level Questions Data (Questions 3.1 and 3.1.1) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015	10%
	Privileged Users CAP Goal	Percent of privileged users that are required to log on to the network with a two-factor PIV card or NIST Level of Assurance 4 credential.	FISMA Agency Level Questions Data (Questions 3.2 and 3.2.1) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015	22%
Anti-Phishing and Malware Defense	Anti-Phishing Defense CAP Goal	The lowest implementation percentage of the top five capabilities from among the seven anti-phishing capabilities. Capabilities include: analyzing incoming email for clickable URLs, embedded content, and attachments; opening of email attachments in a sandboxed environment; using sender authentication protocols; scanning incoming emails using a reputation filter; using filtration technology for inbound email traffic; the capability to digitally sign email; and users successfully completing exercises focused on phishing.	FISMA Agency Level Questions Data (Questions 4.2, 4.5, 4.6, 4.7, 4.9, 4.13 and 8.2.1) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015	33%

Key performance area	Sub-performance area	Definition	Source	Non-CFO Act Agency Performance Average
	Malware Defense CAP Goal	The lowest implementation percentage of the top three capabilities from among the five malware defense capabilities. The capabilities measure hardware assets for: host-based intrusion prevention systems; antivirus solutions that use file reputation services; anti-exploitation tools; browser-based or enterprise-based tools to block known phishing websites; the percent of remote access solutions that scan for malware upon connection.	FISMA Agency Level Questions Data (Questions 4.3, 4.4, 4.8, 4.11 and 6.1.4) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015	53%
	Other Defense CAP Goal	The lowest implementation percentage of the top two capabilities from among the four other defense capabilities. The capabilities measure the percent of privileged user accounts that have a technical control preventing internet access; the percent of inbound network traffic that passes through a web content filter; outbound communications traffic checked to detect covert exfiltration of information; percent of email traffic on systems that have the capability to quarantine or otherwise block email.	FISMA Agency Level Questions Data (Questions 4.1, 4.10, 4.12 and 4.14) reported to DHS via CyberScope from October 1, 2014, to September 30, 2015	66%

APPENDIX 3: IT SECURITY SPENDING REPORTED BY CFO ACT AGENCIES

Over the fiscal next year, the Administration will continue to commit considerable resources to strengthen Federal cybersecurity, including modernizing or replacing antiquated technology, streamlining disparate IT budgeting and governance structures, and closing cybersecurity workforce shortages and skill gaps. Additionally, Federal agencies must devote significant resources to secure Federal information systems, networks, and data. Each year, OMB requires agencies to report cybersecurity-spending data to determine agency-specific cybersecurity needs.

In FY 2015, all CFO Act agencies reported spending in these functions:

Prevent Malicious Cyber Activity

This area contains categories of spending dedicated to monitoring Federal Government systems and networks and protecting the data within from both external and internal threats. Such categories include:

- Trusted Internet Connections;
- Intrusion prevention systems;
- User identity management and authentication;
- Supply chain monitoring;
- Network and data protection;
- Counterintelligence; and
- Insider threat mitigation activities.

Detect, Analyze, and Mitigate Intrusions

This area contains spending on systems and processes used to detect security incidents, analyze the threat, and attempt to mitigate possible vulnerabilities. These categories include:

- Computer Emergency Response Teams;
- Federal Incident Response Centers;
- Cyber threat analysis;
- Law enforcement;
- Cyber continuity of operations;
- Incident response and remediation;
- Forensics and damage assessment;
- ISCM and IT security tools; and
- Annual FISMA testing.

Shaping the Cybersecurity Environment

This area contains categories of spending designed to improve the efficacy of current and future information security efforts, including building a strong information security workforce and supporting broader IT security efforts. These categories include:

- National Strategy for Trusted Identities in Cyberspace;
- Workforce development;
- Employee security training;

- Standards development and propagation;
- International cooperation activities; and
- Information security and assurance research and development.

Table 42: IT Security Spending Reported by CFO Act Agencies

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shaping the Cybersecurity Environment	Total
Department of Agriculture	$39	$39	$5	$83
Department of Commerce	$43	$79	$71	$194
Department of Education	$8	$18	$0	$27
Department of Energy	$130	$105	$68	$303
Department of Justice	$291	$131	$35	$456
Department of Labor	$6	$12	$4	$22
Department of State	$102	$73	$25	$200
Department of Transportation	$41	$49	$5	$95
Department of Veterans Affairs	$96	$89	$25	$210
Department of the Interior	$13	$20	$28	$61
Department of the Treasury	$159	$96	$16	$271
Department of Defense	$3,200	$1,100	$4,800	$9,100
Department of Health & Human Services	$71	$132	$17	$220
Department of Homeland Security	$316	$771	$225	$1,313
Department of Housing & Urban Development	$7	$8	$1	$15
Environmental Protection Agency	$2	$12	$3	$17
General Services Administration	$16	$24	$6	$46
International Assistance Programs	$8	$8	$5	$22
National Science Foundation	$3	$6	$206	$215
National Aeronautics & Space Administration	$30	$54	$23	$107
Nuclear Regulatory Commission	$8	$13	$3	$25
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$2	$8	$0	$10
Social Security Administration	$51	$38	$2	$91
Total Cybersecurity Spending	**$4,646**	**$2,887**	**$5,577**	**$13,110**

NOTE: Due to rounding, categories may not sum to the total

APPENDIX 4: INSPECTORS GENERAL INDEPENDENT ASSESSMENTS

As described in Section III, each agency's Inspector General (IG) assessed their department's information security programs in the ten areas outlined below. Section III also notes how many agencies had programs in each of the areas. The following two sections summarize the results in each of the program areas focusing on programs that were in place.

The Ten Cyber Security Areas—CFO Act Agencies
The results for the cybersecurity areas are summarized below for the CFO Act agencies.[1]

Information Security Continuous Monitoring (ISCM):

ISCM and adjustment of security controls are essential to protect systems. Security personnel need the real-time security status of their systems, and management needs up-to-date assessments in order to make risk-based decisions. ISCM has become a key focus for improving Federal information security and provides the required real-time view into security control operations.

For the FY 2015 FISMA review, the Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency, in coordination with DHS, OMB, NIST, and other key stakeholders, developed a maturity model to provide perspective on the overall status of information security continuous monitoring program within an agency. The maturity model summarizes the status of the program based on a 5-level maturity scale from lowest to highest: Level 1 (Ad Hoc), Level 2 (Defined), Level 3 (Consistently Implemented), Level 4 (Managed and Measurable), and Level 5 (Optimized). To reach a particular level of program maturity, organizations should meet all of the requirements for people, process, and technology domains for that level. The overall maturity of the organization's ISCM program would be based on the lowest level identified for each of the domains.

Based on the Inspectors General's reviews, 15 of the 23 agencies are in the lowest level of maturity ("ad hoc"), while only eight IGs reported that his or her department had all of the requirements to move to the next maturity level.

- Maturity Level 1 (Ad Hoc): The ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS (15 departments);
- Maturity Level 2 (Defined): The ISCM program has developed comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide (six departments); and,

[1] Due to the size of the Department, the DOD OIG is unable to definitively report a yes or no answer for all FISMA attributes.

- Maturity Level 3 (Consistently Implemented): In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS (two departments).

Configuration Management:

To secure both software and hardware, departments must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. OMB requires all workstations that use Windows to conform to the U. S. Government Configuration Baseline. Furthermore, NIST has created a repository of secure baselines for a wide variety of operating systems and devices.

Based on the IGs' reviews, 16 agencies had configuration management programs in place. However, only two IGs reported that their department had all of the requirements of a successful configuration management program. The following deficiencies were most common:

- Assessments of compliance with baseline configurations are not performed (five departments);
- The department does not have a process for timely (as specified in organization policy or standards) remediation of scan result deviations (five departments);
- Software assessment (scanning) capabilities were not fully implemented (four departments);
- Configuration-related vulnerabilities, including scan findings, had not been remediated in a timely manner (12 departments);
- Patch management process was not fully developed, including a process for timely and secured installation of software patches (five departments);
- The organization does not have an enterprise deviation handling process and it is not integrated with an automated scanning capability (four departments); and,
- There is no process for mitigating the risk introduced by approved deviations (four departments).

Identity and access management:

Proper identity and access management ensures that users and devices are properly authorized to access information and information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, and the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. HSPD-12 calls for all Federal departments to require personnel to use PIV cards. This use of PIV cards is a major component of a secure, government-wide account and identity management system.

Seventeen IGs reported that their departments had identity and access management programs in place. However, not all metrics were met. The most common control weaknesses were:

- The department did not plan for implementation of PIV for logical access (three departments);
- The department did not ensure that the users are granted access based on needs and separation of duties principles (six departments); and,

- The department did not ensure that accounts were terminated or deactivated once access was no longer required (eight departments).

Incident response and reporting:

Information security incidents occur on a daily basis. Departments must have sound policies and planning in place to respond to these incidents and report them to the appropriate authorities. OMB M-06-19 designated US-CERT to receive reports of incidents on unclassified Federal Government systems, and requires the reporting of incidents that involve sensitive data, such as personally identifiable information, within strict timelines.

Incident response and reporting programs were largely compliant. Nineteen IGs reported that their departments had incident response and reporting programs in place. However, five IGs identified at least one missing component. The following deficiencies were most common:

- The department does not complete a comprehensive analysis, or validate and document incidents (three departments);
- The department does not report to law enforcement within established timeframes (three departments); and,
- The department does not respond to and resolves incidents in a timely manner to minimize further damage (four departments);

Risk management:

Every information technology system presents risks, and security managers must identify, assess, and mitigate their systems' risks. Federal executives rely on accurate and continuous system assessments since they are ultimately responsible for any risks posed by their systems' operations.

Thirteen IGs reported that their departments had risk management programs in place. However, only three of the 13 reported complete programs, while ten identified at least one missing component. The following deficiencies were most common:

- The department did not have an up-to-date system inventory (four departments);
- The department did not implement the tailored set of baseline security controls and describe how the controls are employed within the information system and its environment of operation (four departments);
- The department does not implement the approved set of tailored baseline security controls that were identified (four departments);
- The department did not assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (five departments);
- The department does not have an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status (four departments); and,
- For cloud systems, the organization cannot identify the security controls, procedures, policies, contracts, and service level agreements in place to track the performance of the CSP and manage the risks of Federal program and personal data stored on cloud systems (six departments).

Security training:

FISMA requires all Federal Government personnel and contractors to complete annual security awareness training that provides instruction on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, departments cannot ensure that all personnel receive the required training.

Nineteen IGs reported that their departments had compliant programs. Eight reported that their departments' programs included all of the required elements. Among the eleven incomplete programs, the following deficiencies were most common:

- Identification and tracking of the status of security awareness training was not complete for all personnel (employees, contractors, and other organization users) with access privileges that require the training (four departments); and,
- Identification and tracking of the status of specialized training was not completed for all personnel with significant information security responsibilities that required specialized training (nine departments).

Plan of Action & Milestones (POA&M) Remediation:

When agencies identify weaknesses in information security systems as the result of controls testing, audits, incidents, continuous monitoring, or other means, it must record each weakness with a POA&M. This plan provides security managers, accreditation officials, and senior officials with information on the overall risk posed to the system. This takes into account the type of weakness, actions planned to address risk, associated costs, and expected completion dates.

Eighteen IGs reported that their departments had POA&Ms in place. Of these 18, six also indicated that their departments' programs had all of the required attributes. Of the 12 IGs indicating that their programs need improvements, these following issues were most common:

- The department did not track, prioritize and remediate weaknesses (four departments);
- The department did not ensure remediation plans were effective for correcting weaknesses (four departments);
- The department had not established and adhered to milestone remediation dates (nine departments);
- The department did not develop POA&Ms for security weaknesses discovered during assessments of security controls that require planned mitigation (five departments); and,
- The department did not associate costs with remediating weaknesses and are identified in terms of dollars (seven departments).

Remote access management:

Secure remote access is essential to a department's operations because the proliferation of system access through telework, mobile devices, and information sharing means that information security is no longer confined within system perimeters. Departments also rely on remote access as a critical component of contingency planning and disaster recovery. Each method of remote access requires protections, such as multi-factor authentication that are not required for local access.

Twenty-one IGs reported that their departments had remote access management programs in place, and 14 of these had all requirements. The remaining IGs reported that their departments were missing at least one requirement of a remote access management program. The most common remote access weaknesses were:

- The department authentication mechanism does not meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms (two departments);
- The department does not define and implement encryption requirements for information transmitted across public networks (two departments); and,
- Remote access sessions are not timed-out after 30 minutes of inactivity, after which re-authentication is required (three departments).

Contingency planning:

FISMA requires Federal departments to prepare for events that may affect the availability of an information resource. This preparation entails identification of resources and risks to those resources, and the development of a plan to address the consequences if harm occurs. Consideration of risk to a department's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. Critical systems may require redundant sites that run 24 hours a day/7 days a week, while less critical systems may not be restored at all after an incident. Once a contingency plan is in place, training and testing must be conducted to ensure that the plan will function in the event of an emergency.

Eighteen IGs reported that their departments had contingency planning programs in place. However, only six reported that their departments' contingency planning programs were fully compliant with standards. The following issues were prevalent among the 12 departments that needed improvements:

- The department has not incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (six departments);
- The department did not conduct testing of system-specific contingency plans (five departments);
- The department did not have documented Business Continuity Plan and Disaster Recovery in place for implementing when necessary (four departments);
- The department did not develop a test, training, and exercise program (four departments); and,
- The department's alternate processing sites are not subject to the same risks as primary sites (seven departments).

Contractor systems:

Contractors and other external entities own or operate many information systems on behalf of the Federal Government, including systems that reside in the public cloud. These systems must meet the security requirements for all systems that process or store Federal Government information. Consequently, these systems require oversight by the departments that own or use them to ensure that they meet all applicable requirements.

Sixteen IGs reported that their departments had programs in place to manage contractor systems, but only eight reported that their departments' programs included all requirements. Eight IGs

reported that their departments' programs lacked at least one required element. The most common weaknesses reported were:

- The department did not obtain sufficient assurance that security controls of such systems and services were effectively implemented and complied with Federal and organization guidelines (six departments);
- The department did not have a complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud (five departments);
- The department inventory does not identify interfaces between these systems and organization-operated systems (four departments); and,
- The department does not require appropriate agreements (e.g. MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates (four departments).

The Ten Cybersecurity Areas—Small Agencies

The results for the cybersecurity areas are summarized for small agencies.

ISCM:

Based on the IGs' reviews, 25 of the 47 are in the lowest level of maturity ("ad hoc"), while 19 IGs reported that their agencies had all of the requirements to move to the next maturity level. Specifically, 16 agencies were at Level 2, while only three agencies reached Level 3 or above.

Configuration Management:

Based on the IGs' reviews, 24 agencies had configuration management programs in place. However, only 11 IGs reported that their agencies had all of the requirements of a successful configuration management program. The following deficiencies were most common:

- The agency does not have a process for timely (as specified in organization policy or standards) remediation of scan result deviations (four agencies);
- The department has not implemented software assessing (scanning) capabilities (five agencies);
- Configuration-related vulnerabilities, including scan findings, had not been remediated in a timely manner (four agencies); and,
- The organization does not have an enterprise deviation handling process and it is not integrated with an automated scanning capability (six agencies).

Identity and access management:

Thirty IGs reported that their agencies had identity and access management programs in place. Sixteen of these reported that their agencies' programs lacked at least one required element. The most common control weaknesses were:

- The agency did not plan for implementation of PIV for logical access (nine agencies);
- The agency did not ensure that the users are granted access based on needs and separation of duties principles (seven agencies); and,

- The agency did not ensure that accounts were terminated or deactivated once access was no longer required (eight agencies).

Incident response and reporting:

Incident response and reporting programs were largely compliant. Thirty-four IGs reported that their agencies had incident response and reporting programs in place. However, 12 IGs identified at least one missing component. The following deficiencies were most common:

- The department does not complete a comprehensive analysis, or validate and document incidents (three agencies);
- The department does not report to US-CERT within established timeframes (nine agencies); and,
- The agency does not respond to and resolves incidents in a timely manner to minimize further damage (eight departments).

Risk management:

Twenty-four IGs reported that their agencies had risk management programs in place. Of these 24, only 15 reported complete programs and nine reported that most attributes were met.

Security training:

Thirty-four IGs reported that their agencies had compliant programs. Twenty-five reported that their agencies' programs included all of the required elements. Among the nine incomplete programs, the following deficiencies were most common:

- Documented policies and procedures for specialized training for users with significant information security responsibilities do not exist (six agencies);
- Security training content is not based on the organization and roles, as specified in organization policy or standards (three agencies); and,
- Identification and tracking of the status of specialized training was not completed for all personnel with significant information security responsibilities that required specialized training (three agencies).

POA&M Remediation:

Thirty IGs reported that their agencies had POA&Ms in place. Seventeen indicated that their agencies' programs had all of the requirements. The following issues were the most common for the 13 IGs indicating that existing programs needed improvement:

- The department had not established and adhered to milestone remediation dates (seven agencies);
- The department does not associate cost with remediating weaknesses in terms of dollar (ten agencies); and,

Program officials do not report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO does not centrally track, maintain, and independently review/validate POA&Ms (four agencies).

Remote access management:

Thirty-two IGs reported that their agencies had remote access management programs in place, and 18 of these had all requirements. The remaining IGs reported that their agencies were missing at least one requirement of a remote access management program. The most common remote access weaknesses were:

- The department authentication mechanism does not meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms (four agencies);
- The department does not define and implement encryption requirements for information transmitted across public networks (four agencies);
- Remote access sessions are not timed-out after 30 minutes of inactivity, after which re-authentication is required (six agencies); and
- Training material for security awareness training does not contain appropriate content for the organization (seven agencies).

Contingency planning:

Thirty-one IGs reported that their agencies had contingency planning programs in place. However, only nineteen reported that their agencies contingency planning programs were fully compliant with standards. The following issues were prevalent among the 12 agencies that needed improvements:

- The department did not conduct testing of system-specific contingency plans (six agencies);
- The department has not developed test, training, and exercise (TT&E) programs (four agencies);
- The department has not conducted testing or exercising BCP and DRP to determine effectiveness and to maintain current plans (six agencies);
- The departments' after action reports do not address issues identified during contingency/disaster recovery exercises (five agencies); and,
- The department's alternate processing sites are not subject to the same risks as primary sites (eight agencies).

Contractor systems:

Twenty-seven IGs reported that their agencies had programs in place to manage contractor systems, and 19 reported that their agencies' programs included all requirements. Eight of the 27 IGs reported that their agencies' programs lacked at least one required element. The most common weakness reported was:

- The department did not obtain sufficient assurance that security controls of such systems and services were effectively implemented and complied with Federal and organization guidelines (five agencies.).

APPENDIX 5: LIST OF CFO ACT AGENCIES

CFO Act Agency	Acronym
Department of Agriculture	USDA
Department of Commerce	Commerce
Department of Defense	DOD
Department of Education	ED
Department of Energy	Energy
Department of Health and Human Services	HHS
Department of Homeland Security	DHS
Department of Housing and Urban Development	HUD
Department of the Interior	Interior
Department of Justice	Justice
Department of Labor	Labor
Department of State	State
Department of Transportation	DOT
Department of the Treasury	Treasury
Department of Veterans Affairs	VA
U.S. Agency for International Development	USAID
Environmental Protection Agency	EPA
General Services Administration	GSA
National Aeronautics and Space Administration	NASA
National Science Foundation	NSF
Nuclear Regulatory Commission	NRC
Office of Personnel Management	OPM
Small Business Administration	SBA
Social Security Administration	SSA

Source: *Chief Financial Officers Act of 1990 (P.L. 101-576)*

APPENDIX 6: LIST OF NON-CFO ACT AGENCIES REPORTING TO CYBERSCOPE

The following agencies submitted FISMA data for this report through CyberScope. CyberScope is a data reporting application developed by DHS and Justice to handle manual and automated inputs of agency data for FISMA compliance reporting.

Non-CFO Act Agency	Acronym
Advisory Council on Historic Preservation	ACHP
Armed Forces Retirement Home	AFRH
Barry Goldwater Scholarship and Excellence in Education Foundation	BGSEEF
Broadcasting Board of Governors	BBG
Chemical Safety Board	CSB
Commission of Fine Arts	CFA
Commission on Civil Rights	USCCR
Committee for Purchase from People Who Are Blind or Severely Disabled	CPPBSD
Commodity Futures Trading Commission *	CFTC
Consumer Financial Protection Bureau *	CFPB
Consumer Product Safety Commission *	CPSC
Corporation for National and Community Service	CNCS
Court Services and Offender Supervision Agency	CSOSA
Defense Nuclear Facilities Safety Board	DNFSB
Denali Commission	DENALI
Election Assistance Commission	EAC
Equal Employment Opportunity Commission	EEOC
Export-Import Bank of the United States	EXIM
Farm Credit Administration †	FCA
Federal Communications Commission	FCC
Federal Deposit Insurance Corporation *	FDIC
Federal Election Commission *	FEC
Federal Energy Regulatory Commission *	FERC
Federal Housing Finance Agency *	FHFA
Federal Labor Relations Authority	FLRA
Federal Maritime Commission	FMC
Federal Mediation and Conciliation Service	FMCS
Federal Reserve Board *	FRB
Federal Retirement Thrift Investment Board	FRTIB
Federal Trade Commission *	FTC
Institute of Museum and Library Services	IMLS
Inter-American Foundation	IAF
International Boundary and Water Commission	IBWC
International Trade Commission	USITC

Non-CFO Act Agency	Acronym
Merit Systems Protection Board	MSPB
Millennium Challenge Corporation	MCC
Morris K. Udall Foundation	MKUSENEP
National Archives and Records Administration	NARA
National Capital Planning Commission	NCPC
National Credit Union Administration	NCUA
National Endowment for the Arts	NEA
National Endowment for the Humanities	NEH
National Labor Relations Board *	NLRB
National Mediation Board	NMB
National Transportation Safety Board	NTSB
Nuclear Waste Technical Review Board	NWTRB
Occupational Safety and Health Review Commission	OSHRC
Office of Navajo and Hopi Indian Relocation	ONHIR
Office of Special Counsel	OSC
Overseas Private Investment Corporation	OPIC
Peace Corps	PC
Pension Benefit Guaranty Corporation	PBGC
Postal Regulatory Commission	PRC
Privacy and Civil Liberties Oversight Board	PCLOB
Railroad Retirement Board	RRB
Securities and Exchange Commission *	SEC
Selective Service System	SSS
Smithsonian Institution	SI
Tennessee Valley Authority	TVA
United States Access Board	USAB

* Independent Regulatory Agency (44 USC 3502(5))

APPENDIX 7: ACRONYMS

Acronym	
AP	Administrative Priority
ATO	Authority to Operate
BOD	Binding Operational Directive
CAP	Cross Agency Priority
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CNAP	Cybersecurity National Action Plan
CSIP	Cybersecurity Strategy Implementation Plan
CSP	Cloud Service Provider
DoS	Denial of Service
HSPD-12	Homeland Security Presidential Directive 12
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
ITMF	Information Technology Modernization Fund
JAB	Joint Authorization Board
KFM	Key FISMA Metric
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NSC	National Security Council
OFCIO	Office of the Federal Chief Information Officer
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
US-CERT	United States Computer Emergency Response Team

END NOTES

[1] This office was established in accordance with Section 101 of the E-Government Act of 2002, now codified at 44 U.S.C. § 3602, and is headed by the FCIO; this office was previously known as the Office of E-Government and Information Technology (E-Gov).

[2] As described in *OMB Memorandum M-16-03*, 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.

[3] The information types that law, Federal regulations, and government-wide policies currently require agencies to protect may be found listed in the online Controlled Unclassified Information Registry (*https://www.archives.gov/cui*). However, agencies should not start marking and designating their unclassified information as Controlled Unclassified Information pursuant to Executive Order 13556 until the National Archives and Records Administration issues their final guidance to implement EO 13556 and establishes implementation deadlines.

[4] Per M-16-03, Any record that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in a significant or demonstrable impact onto agency mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. A collection of records of special importance in the aggregate could be considered an agency High Value Asset.

[5] In FY 2015, Security Capital Planning will no longer be considered a cybersecurity area for purposes of populating CyberScope, leaving 10 program areas.

[6] DHS, pursuant to the authority provided by OMB, issued the FY 2015 Inspector General FISMA Reporting Metrics on June 19, 2015. This document includes general instructions as well as the 87 attributes.