ANNUAL REPORT TO CONGRESS:

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

OFFICE OF MANAGEMENT AND BUDGET

May 1, 2014

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

DEPUTY DIRECTOR
FOR MANAGEMENT

May 1, 2014

The Honorable Thomas R. Carper
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 Title III of the E-Government Act of 2002 (P.L. 107-347), which requires the Office of Management and Budget (OMB) to submit an annual report on implementation by Federal agencies of the Federal Information Security Management Act of 2002 (FISMA). This report covers October 1, 2012 to September 30, 2013 and provides an update of ongoing information security initiatives, a review of Fiscal Year 2013 information security incidents, Inspector General assessments of agencies' progress in implementing information security capabilities, and the government's progress in meeting key information security performance measures.

This report includes information provided by Federal agencies to OMB and, as you will note, progress has been made in key areas of information security. OMB continues to work with agencies to fulfill the requirements of FISMA and implement increasingly resilient information technology security and privacy management programs.

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

Sincerely,

Beth Cobert
Deputy Director for Management

Enclosure

Identical Letter Sent to:

The Honorable Tom Coburn
The Honorable Elijah Cummings
The Honorable Gene L. Dodaro
The Honorable Lamar Smith
The Honorable John Thune
The Honorable Darrel E. Issa
The Honorable Eddie Bernice Johnson
The Honorable John D. Rockefeller, IV

TABLE OF CONTENTS

SECTION I: INTRODUCTION: CURRENT STATE OF FEDERAL INFORMATION SECURITY

Information technology has evolved rapidly and continues to break new ground with the advancement of virtualization technologies, cloud computing, and mobile devices. Such developments offer opportunities to increase the value and accessibility of government resources and encourage greater internal and external collaboration, but they also expose government information and systems to new and constantly changing threats. As the sophistication and volume of cyber-attacks continue to grow, it is important for the Federal Government to implement policies and procedures to reduce information security risks to a level commensurate with the sensitivity and criticality of information and corresponding information systems.

The *Federal Information Security Management Act of 2002* (P.L. 107-347) (FISMA)[i] provides a comprehensive framework for supporting the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA requires the Office of Management and Budget (OMB) to provide an annual report to Congress outlining the progress of Federal information security efforts as well as deficiencies and the actions taken to correct them. FISMA also requires OMB to develop and oversee the implementation of policies, principles, standards, and guidelines on information security that are commensurate with the risk and magnitude of the possible harm to Federal systems or information. To ensure uniformity in this process, FISMA requires the National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems. In 2010, *OMB Memorandum M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* [ii] expanded the role of DHS in regards to the operational aspects of Federal agency cybersecurity and information systems that fall within FISMA. FISMA also charged OMB with producing an annual report to keep Congress apprised of Federal progress in increasing information security.

While the sophistication and diversity of threats to government systems and information continue to increase, departments and agencies are demonstrating progress in implementing solutions designed to mitigate their risk. The following key indicators (described in more detail in Section III) demonstrate this improvement:

- The governmentwide averages of FISMA capabilities from Fiscal Year (FY) 2012 to FY 2013 have increased from 73% to 81% compliance, with significant improvements in areas such as the adoption of automated configuration management, remote access authentication, and email encryption.

- Cross-Agency Performance (CAP) Goal strategies (trusted internet connections, information security continuous monitoring, and strong authentication) have shown improvement from 77% compliance in FY 2012 to 81% in FY 2013.

In addition to agency progress in these priority areas, in FY 2013 the Federal Government began the transition to automated diagnostics and monitoring. In November 2013, OMB released *Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems."* [iii] The goal of this policy is to provide agencies with a policy framework to: monitor their systems on an ongoing basis; evolve from static reauthorizations, or determinations and acceptance of information security risk, to ongoing authorizations of information systems; and create the technological infrastructure to accomplish continuous diagnostics and mitigation and ongoing authorizations.

These and other initiatives, actions, and metrics, are described in detail throughout this report, which covers the period of October 1, 2012, to September 30, 2013. This report is organized as follows:

Section II: Key Ongoing Information Security Initiatives

Describes the efforts being undertaken to protect government data and IT infrastructure assets, support the safe and secure adoption of emerging technology, and building a 21st century workforce;

Section III: Key Security Metrics

Presents the metrics used to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels.

Section IV: Security Incidents and Response in the Federal Government

Presents information from the United States Computer Emergency Readiness Team (US-CERT) on computer security incidents and Federal efforts to remediate them.

Section V: Summary of Inspectors General's Findings

Provides an overview of the assessments of agency inspectors general (IG) regarding his or her department's information security programs.

Section VI: Progress in Meeting Key Privacy Performance Measures

Provides an overview of the progress made in implementing steps to analyze and address privacy issues.

Section VII: Appendices

Appendix 1: NIST Performance in 2013

Appendix 2: Security Incidents by CFO Act Agency

Appendix 3: Information Security Spending Reported by CFO Act Agencies

Appendix 4: Inspector General's Response

Appendix 5: List of CFO Act Agencies

Appendix 6: List of Non-CFO Act Agencies Reporting to CyberScope

SECTION II: KEY ONGOING INFORMATION SECURITY INITIATIVES

As the Federal Government moves further into the 21st century, agencies face an ever-evolving landscape of information security challenges. Based on information reported by the DHS United States Computer Emergency Readiness Team (US-CERT), and described in more detail in Section IV, malicious code is the most widely reported incident type across all reporting entities. These attacks, which are increasingly sophisticated, often take advantage of flaws in software code or use exploits that can circumvent signature-based tools that commonly identify and prevent known threats. US-CERT and the National Security Agency (NSA) also both identified phishing as a continued and evolving threat, with attackers employing social engineering techniques designed to trick the unsuspecting user to click a malicious link or open a malicious attachment thereby giving an attacker direct access to the Federal Government network.

In order to ensure the continued safety of Federal systems, the Government has undertaken several comprehensive information security initiatives. These initiatives can be categorized as:

- Protecting existing information and information systems;
- Supporting the safe and secure adoption of emerging technology; and
- Building a sophisticated information security workforce.

Through the efforts of these three categories of initiatives, the Federal Government can mitigate the threats that inevitably accompany advances in technology. The Federal Government has made it a priority to protect systems and information from threats like malicious code attacks through the utilization of both technical capabilities and cooperative frameworks. As the Government expands upon these capabilities, it must remain cognizant of supporting the adoption of emerging technologies in a secure manner to reduce the threat of compromising sensitive information. In order to implement both of these efforts, the Government will require a strong information security workforce that is able operate in the increasingly complicated digital environment. While threats to Federal systems and information will continue to evolve, utilizing the three-pronged approach indicated above will ensure that Federal capabilities will evolve as well.

A. PROTECTING EXISTING INFORMATION AND INFORMATION SYSTEMS

Enhanced IT capabilities allow the Government to expand citizens' access to information and services. With this expanded access to information and information systems, the government's risk profile increases. Recognizing the importance of safeguarding government information and information systems, the Administration designated cybersecurity as a Cross Agency Priority (CAP) Goal, increasing senior government officials' visibility of and accountability for this issue. The Cybersecurity CAP Goal encompasses three strategies to safeguard government networks:

- Trusted Internet Connections (TICs);
- Information security continuous monitoring; and
- Strong authentication (HSPD-12).

Each of these strategies aids agencies in improving cybersecurity capabilities to provide safe, secure, and effective mission execution and services. The assessment period for these strategies is FY 2012 through FY 2014. Through the end of FY 2014, the implementation of these strategies will be assessed on a quarterly basis and published on *www.Performance.gov*. The FY 2014 FISMA Report will identify the updated Cybersecurity CAP goal, which will be assessed from FY 2015 through FY 2017. Agencies are held accountable for their CAP and overall information security performance through CyberStat review sessions. These sessions bring senior White House and agency officials together to discuss agency information security performance and associated remediation strategies to improve deficiencies. The CAP goal strategies and associated CyberStat model are described in more detail below.

Trusted Internet Connections (TIC)

The TIC initiative seeks to improve the Federal Government's security posture and increase its incident response capability by optimizing and standardizing the security of individual external network connections, including connections to the Internet. To achieve this, the Government has sought to consolidate external telecommunications connections, establish a set of baseline capabilities through enhanced monitoring, and maintain situational awareness of all external network connections.[iv] In pursuit of this goal, the Government has established access providers to manage the operation of TICs, called TIC Access Providers (TICAPs). Each TICAP has baseline security capabilities designed to protect Federal systems and information, including firewalls, malware policies, and network/security operation centers. An intrusion detection system is also being deployed at each TICAP. This system alerts US-CERT when a specific cyber threat is detected, which allows US-CERT to analyze and react to malicious activity occurring across the Federal IT infrastructure.[v]

Throughout FY 2010 and FY 2011, DHS worked with an inter-agency group of subject matter experts to update the TIC baseline security capabilities based on evolving and increasingly sophisticated threats. The result was TIC Reference Architecture 2.0, or TIC v2.0, which introduced new critical security capability requirements and clarified existing ones. As of September 30, 2012, all executive branch civilian departments and agencies and Managed Trusted Internet Protocol Services (MTIPS) providers, which provide TIC-compliant managed security services, are assessed on TIC v2.0 critical capabilities. In FY 2013, DHS worked with agencies to develop a TIC v2.0 supplemental document focusing on cloud services compliance with TIC. DHS also worked with the CIO Council to develop and release the *Mobile Security Reference Architecture* in May 2013, a document designed to assist the Federal Government procure and manage mobile devices, applications, and data in smart, secure, and affordable ways.[vi]

One of DHS's key technologies for furthering TIC goals is the National Cybersecurity Protection System's (NCPS) EINSTEIN system. The goal of EINSTEIN is to provide the Federal Government with an early warning system, improved situational awareness of intrusion threats to Federal Executive Branch civilian networks, near real-time identification of malicious cyber activity, and prevention of that malicious cyber activity. As noted in the *FY 2012 Federal Information Security Management Act (FISMA) Report*, FY 2013 saw the deployment of intrusion prevention as a managed security service. Through this offering, termed EINSTEIN 3 Accelerated (E3A), the government seeks to gain an intrusion prevention capability with the ability to block and disable attempted intrusions before any harm can be done. By contracting with major Internet Service Providers (ISPs), E3A leverages private sector cybersecurity innovation enhanced by data that is uniquely held by the Federal Government. The initial deployment of E3A is focused on countermeasures that will address 85% of the cybersecurity

threats affecting the Executive Branch civilian networks.[vii] DHS awarded its first ISP contract for E3A services in March 2013. For FY 2014, the DHS Office of Cybersecurity and Communications will continue with the rollout of E3A and securing memorandums of agreement (MOAs) with all departments and agencies.

Information Security Continuous Monitoring (ISCM)

ISCM is an existing and expanding initiative for combatting information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. As noted above, OMB released *Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems"* in November 2013. The goals of this memorandum were to provide agencies with a policy framework to:

- Monitor their systems on an ongoing basis;
- Evolve from static reauthorizations to ongoing authorizations of information systems; and
- Create the technological infrastructure to accomplish ISCM and ongoing authorizations.

In conjunction with the release of M-14-03, DHS established the Continuous Diagnostics and Mitigation (CDM) Program. Under this program, DHS coordinated with the General Services Administration (GSA) to establish a governmentwide Blanket Purchase Agreement (BPA), which Federal, state, local and tribal governments can leverage to deploy a basic set of capabilities to support continuous monitoring of security controls in Federal information systems and environments of operation.[viii] The BPA, awarded on August 12, 2013, provides a consistent, governmentwide set of ISCM tools to enhance the Federal Government's ability to identify and respond, in near real-time, to the risk of emerging cyber threats. It also capitalizes on strategic sourcing to minimize the costs associated with implementing requirements of the Risk Management Framework.

Strong Authentication: HSPD-12

Homeland Security Presidential Directive 12 (HSPD-12), issued in August 2004, is a strategic initiative that requires agencies to follow specific technical standards and business processes for the issuance and routine use of Federal PIV smartcard credentials, including a standardized background investigation to verify employees' and contractors' identities.[ix] The goal of the initiative is to ensure that only authorized personnel have access to government systems and applications. This creates a more secure enterprise architecture by reducing the opportunity for identity fraud, thereby increasing the safety of both government information and personal privacy.

The *2009 Cyberspace Policy Review*, issued at the direction of the President, highlighted the importance of identity management in protecting the nation's infrastructure.[x] In 2012, the Administration identified HSPD-12 as a strategy within the cybersecurity CAP Goal. Over the past year, the Federal Government continued to focus on leveraging the electronic capabilities of the PIV cards, which have been issued to almost 5.4 million Federal employees and contractors. *OMB Memorandum M-11-11, "Continued Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,"* [xi] issued in February 2011, required each agency to develop and issue an implementation policy through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.

In September 2013, NIST issued revision two of the HSPD-12 standard, *Federal Information Processing Standard (FIPS) 201,*[xii] to address the integration of PIV credentials with mobile devices and advances in technology. Additionally, NIST is working on a new Special Publication 800-157, "Guidelines for Personal Identity Verification (PIV) Derived Credentials," which will increase information security by providing alternative authentication solutions for technology like mobile devices where the use of a PIV card for network access would be impractical.

CyberStat

In order to monitor agency performance in CAP goal implementation and other information security initiatives, DHS, in coordination with OMB and the National Security Council (NSC) established CyberStat review sessions. CyberStat reviews are face-to-face, evidence-based meetings to ensure agencies are accountable and working towards continued improvement of their cybersecurity posture. At the same time, these reviews are meant to assist departments and agencies in developing specific strategies for improving information security.

In FY 2013, DHS selected seven CyberStat participant agencies based on an analysis of self-reported data that identified weaknesses or challenges to the department or agency security posture. The CyberStat reviews provided the agencies opportunity to identify the cybersecurity capability areas where they were facing implementation maturity challenges. The top challenges raised by agencies included: organizational structure and culture; technology (e.g., the need to upgrade legacy systems to support new capabilities); internal process (e.g., distributed budget authority); acquiring skilled staff; and ensuring that the necessary financial resources are allocated to the Administration's priority initiatives for cybersecurity. These reviews assisted agencies in successfully focusing their efforts on issues such as increased HSPD-12 implementation, an area in which one agency expected to see a 6% increase in deployment in 2014, or TIC traffic consolidation, an area in which some agencies saw increases of more than 20%. In addition, CyberStat reviews highlighted areas where agencies are meeting and exceeding requirements, which enabled DHS to utilize their successes to disseminate best practices to other agencies.

In addition to CyberStat reviews, DHS continues to assess both operational readiness and the cybersecurity risk of unclassified networks and systems by proactively engaging Federal audiences to conduct risk and vulnerability assessments. This is done by deploying DHS risk and vulnerability teams to work with agency information security personnel in order to better assess capabilities, identify vulnerabilities, evaluate risks, and provide prioritized guidance that optimizes the remediation activities needed to close capability gaps and limit exposure to threats. The continued use of agency vulnerability assessments will help ensure that agencies maintain ongoing awareness of active threats, and possess the technical expertise to remediate these threats.

Information Sharing and Safeguarding to Prevent Unauthorized Disclosure

While departments and agencies made some progress in improving the security of classified networks during the last reporting period, recent events involving insider threats reinforce the need to continue the work begun under *Executive Order (EO) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."* [xiii] The Senior Information Sharing and Safeguarding Steering Committee (Steering Committee), established under EO 13587, has established clear, consensus-based goals and a plan for measuring progress on classified sharing and safeguarding. In 2013,

the Steering Committee continued to oversee department and agency implementation of initial priorities and developed plans for addressing emerging vulnerabilities on classified systems. These actions will continue to improve the security of our classified information and systems and will enhance the support of our critical national security missions while continuing to promote responsible sharing of classified information.

Continued efforts by the Steering Committee to advance the priority areas will improve security by: strengthening the identification of individuals who are accessing classified systems; limiting access on the basis of the individual's "need-to-know" through technical controls; reducing the opportunity for information to be removed from the secure environment; improving efforts against insider threats; and improving audit capabilities. However, considerable work remains in three priority areas: Reduced Anonymity; Access Control; and Enterprise Audit.

B. SUPPORTING SAFE AND SECURE ADOPTION OF EMERGING TECHNOLOGIES

While the above mentioned initiatives are essential to protect existing systems, attention also must be paid to maintaining information security as new and innovative technologies are utilized to improve information access and service delivery. To this end, the Federal Government is harnessing the transformative power of emerging technologies such as cloud computing, mobile technology, and wireless platforms to efficiently and effectively provide the American public and Federal employees access to information, services and resources. In order to seamlessly integrate these innovative solutions into government operations, the government has engaged in the following initiatives:

- Facilitating Mobile Security
- FedRAMP and the Safe, Secure Adoption of Cloud
- National Security for Trusted Identities in Cyberspace

Through these initiatives, the Government reaps the benefits of technological advances while managing the risk to Federal systems and information. The state of each of these efforts is provided below.

Facilitating Mobile Security

In May 2012, the President signed a memorandum issuing the *Digital Government Strategy*, with the goal of building a 21st century Government by delivering better services to the American people.[xiv] The strategy embraced the need to innovate and architect systems to leverage modern services provided by mobile devices while recognizing that architecting for openness and adopting new technologies has the potential to make devices and data vulnerable to malicious or accidental breaches of security and privacy.

To promote the secure adoption and use of new technologies, an interagency team led by DHS, DOD, and NIST developed a baseline of standard security requirements for mobile computing, a mobile computing decision framework, and a mobile security reference architecture incorporating security and privacy by design. This effort will help Federal executives, program managers, and system owners evaluate the risks associated with the emerging mobile environment needed to support each agency's mission requirements. GSA also announced its *Managed Mobility Program* in May 2013, which identifies potential vendors providing mobile

device management and mobile application management solutions to agencies. GSA and a cross-government team identified a set of Mobile Device Management (MDM) and Mobile Application Management (MAM) functional requirements. The team also identified potential solutions that can both meet those requirements and be procured through existing governmentwide contracts.

In addition to its work on the Digital Government Strategy, NIST issued a series of resources to assist organizations in managing challenges associated with increased use of mobile devices. In June 2013, NIST issued *Special Publication (SP) 800-124 Revision 1, "Guidelines for Managing and Securing Mobile Devices in the Enterprise,"* to help organizations select, implement and use management technologies to secure mobile devices throughout their life cycle. [xv] NIST also issued draft *SP 800-164, "Guidelines on Hardware-Rooted Security in Mobile Devices,"* to provide a common baseline of security technologies that can be implemented across a wide range of mobile devices, helping secure organization-issued and personally-owned devices brought into an organization. [xvi]

The capabilities and small form factors of mobile devices have introduced new identity management challenges. Federal agencies currently authenticate users using the PIV Card deployed, along with its supporting infrastructure, as part of the aforementioned HSPD-12 efforts aimed at enhancing security, promoting interoperability, and increasing government efficiency. Using these cards with mobile devices has proved challenging, and NIST has been working with agencies to identify solutions that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices. In addition to the previously mentioned efforts regarding revision 2 of FIPS 201 (also called FIPS 201-2), and draft SP 800-157, NIST is also updating *SP 800-73, "Interfaces for Personal Identity Verification,"* which will include a new capability for mobile devices to securely use the credentials on the PIV card over a wireless interface, increasing ease of use for users while maintain the security of a PIV card. [xvii]

FedRAMP and the Safe, Secure Adoption of Cloud

To accelerate the adoption of cloud computing solutions across the government, the Administration made cloud computing an integral part of the "Federal Chief Information Officer's *25 Point Implementation Plan to Reform Federal Information Technology Management.*"[xviii] A year later, in 2011, the Federal Cloud Computing Strategy[xix] identified ensuring the safety, security and reliability of data as an important challenge in moving to cloud computing environments. Recognizing this challenge, on December 8, 2011 the Federal CIO published the *"Security Authorization of Information Systems in Cloud Computing Environments"* policy memorandum.[xx] This memorandum formally established the Federal Risk and Authorization Management Program (FedRAMP) and set out roles and responsibilities, implementation timelines, and requirements for agency compliance.

FedRAMP shifted into full operational capability in FY 2013 and is currently helping agencies to accelerate their adoption of secure cloud solutions and substantially lower their costs through the use of standardized security processes, assessments, and authorizations. The program issued eight Joint Authorization Board (JAB) Provisional Authorizations and three Agency Authorizations to Cloud Service Providers (CSPs), for a total of 11 FedRAMP compliant cloud service offerings that agencies can leverage. NIST also issued numerous guidance documents in support of FedRAMP, including the *Federal Cloud Computing Technology Roadmap*, the *Cloud Computing Standards Roadmap*, the *Cloud Computing Reference Architecture*, and the *Cloud Computing Security Reference Architecture*. Related efforts, including updates to *NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations,"* [xxi] have helped accelerate the adoption of cloud computing technologies across

the Federal Government. By June 2014, all cloud services across the government will have to be FedRAMP compliant, a requirement the FedRAMP team will help Federal agencies meet through outreach, education, and direct assistance.

National Security for Trusted Identities in Cyberspace

In response to demand for improved digital identification from the private sector, other levels of government, and the general public, the Administration released the *"National Strategy for Trusted Identities in Cyberspace"* (NSTIC) in April 2011.[xxii] The NSTIC calls for a public-private collaboration to create an Identity Ecosystem – a marketplace of more secure, convenient, interoperable and privacy-enhancing solutions for online authentication and identification. The NSTIC outlines an approach for the Executive Branch to catalyze and facilitate the private sector's development of this online identity environment, in which individuals and organizations can utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Federal Identity, Credential, and Access Management (ICAM) roadmap will continue to guide Federal efforts, while the NSTIC will build off of the principles of the ICAM activities to provide the framework for the broader public and private, national and international efforts.

In support of NSTIC and ICAM, several Federal agencies are working with the United States Postal Service and GSA, who are currently overseeing a Federal Cloud Credential Exchange (FCCX) pilot that will go live in FY 2014. The FCCX will serve as a government operated service that will provide a consistent approach to authentication for citizen facing systems and applications. It will provide a secure, privacy-enhancing, efficient, easy-to-use and interoperable mechanism for government applications to accept Federal ICAM Trust Framework Provider approved, externally issued credentials.

C. BUILDING A SOPHISTICATED INFORMATION SECURITY WORKFORCE

In order to achieve successful implementation of the above initiatives and maintain the future security of government resources, the Federal Government needs to ensure that human resource tools and initiatives are in place to attract and retain capable information security personnel. As described in the *FY 2012 FISMA report*, the *National Cybersecurity Workforce Framework* provides a baseline for organizations within the Federal Government to develop human capital management programs, including defining roles, designing competency models, standardizing job descriptions, and providing specialized training. Using a common language to discuss the work and skill requirements of cybersecurity professionals has enhanced our Nation's ability to baseline capabilities, identify skill gaps, develop cybersecurity talent in the current workforce, and prepare the pipeline of future talent.

The Framework was revised in March 2013, and remains available to the public through NIST's *National Initiative for Cybersecurity Education* (NICE) website, and the *DHS National Initiative for Cybersecurity Careers and Studies* website. These websites provide resources for cybersecurity awareness, education, training, and career information.

In addition, OPM and the Federal Chief Information Officers Council (CIO Council) have expanded their efforts to capitalize on the Framework in support of Federal cybersecurity workforce development. In October 2013, OPM initiated the use of data elements to identify cybersecurity positions to be coded in the Enterprise Human Resources Integration database, an

action that further clarifies the composition and capabilities of the Federal IT civilian workforce executing cybersecurity responsibilities.

SECTION III: KEY SECURITY METRICS

FY 2013 FISMA metrics were designed to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels. These measures were developed through a collaborative effort between OMB, NSC, DHS, and the CIO Council. The baseline established in FY 2012 allows for the measurement of progress in multiple security capability areas both within agencies and across the Federal enterprise. Where agencies require improvement in particular areas, the CyberStat processes, discussed in Section II, will be leveraged to assist in improving agency performance.

This section includes agency specific metrics data reported by CFO Act agencies through CyberScope, an online data collection tool administered by DHS to collect performance data, and summary metrics data reported by non-CFO Act agencies. Additionally, CFO Act agencies reported detailed information security spending data to OMB, which is explained in more detail in Appendix 3.

A. INFORMATION SECURITY METRICS FOR CFO ACT AGENCIES

As agency FISMA reporting has evolved to the aforementioned performance and outcome based model, the establishment of a performance measurement framework to assess agency progress has been essential key development. The following subsections highlight these metrics for the Cyber CAP Goal strategies discussed in Section II as well as other key FY 2013 FISMA metrics that have been derived from Administration priorities (as determined by OMB and the NSC staff). More specific information on each of these metrics is outlined throughout this section, and is also available online at *www.dhs.gov/federal-network-resilience*. The programs discussed in this section are:

- Information Security Continuous Monitoring (ISCM);
- Trusted Internet Connections (TIC);
- Strong Authentication: HSPD-12;
- Portable Device Encryption;
- Domain Name System Security Extensions (DNSSEC) Implementation and Email Validation;
- Remote Access;
- Controlled Incident Detection;
- Security Training;
- Automated Detection and Blocking of Unauthorized Software; and
- Email Encryption.

The FISMA metrics highlighted in Table 1 were built to select the highest impact area for governmentwide application. Table 1 provides a comparison of all FISMA capabilities (both Cyber CAP goal priorities and key FISMA metrics) from FY 2012 to FY 2013. The data shown in Table 1 (with the exception of Domain Name System Security Extensions (DNSSEC) implementation data) was reported by Federal agencies through CyberScope. DNSSEC data are validated values obtained through compliance scans and on-site assessments conducted by DHS. For those metrics that correspond to a broader initiative, the appropriate subsection has been noted below.

Table 1. Comparison of FISMA Capabilities from FY 2012 to FY 2013

Capability Area	FY 2012	FY 2013
Automated Asset Management (ISCM)	86%	83%
Automated Configuration Management (ISCM)	70%	79%
Automated Vulnerability Management (ISCM)	83%	81%
TIC Traffic Consolidation (TIC)	81%	86%
TIC 2.0 Capabilities (Includes Einstein 2) (TIC)	84%	87%
PIV Logical Access (HSPD-12)	57%	67%
Portable Device Encryption	90%	84%
DNSSEC Implementation	74%	93%
E-Mail Validation Technology (DNSSEC)	64%	74%
Remote Access Authentication (Remote Access)	53%	79%
Remote Access Encryption (Remote Access)	82%	98%
Controlled Incident Detection	63%	73%
User Training (Security Training)	88%	94%
Users with Security Responsibility Training (Security Training)	92%	92%
Detect and Block Unauthorized Software	60%	73%
Email Encryption	35%	51%
Governmentwide Average	73%	81%

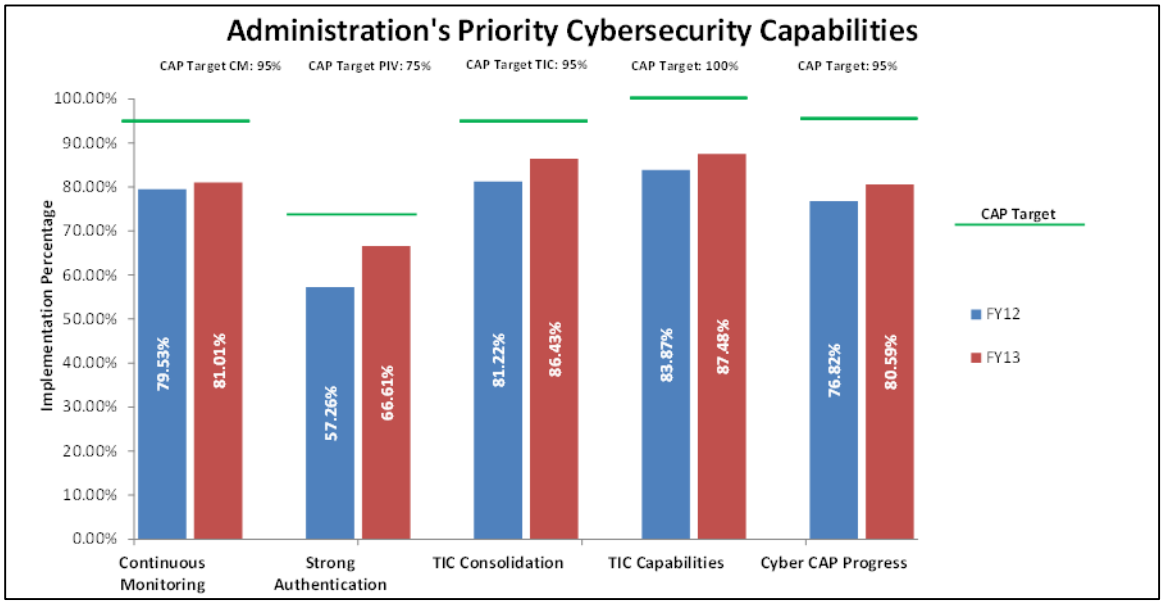
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013, with the exception of DNSSEC data, which is presented as reported by DHS as measured by the DHS Cybersecurity Capability Validation (CCV) tools. For information on how these metrics were derived, please visit:
www.dhs.gov/sites/default/files/publications/FY13%20CIO%20FISMA%20Metrics.pdf

Cyber CAP Goal Performance

As noted in Section II, the Cyber CAP goal is comprised of the following strategies: continuous monitoring, HSPD-12 implementation for logical access, TIC security capabilities and TIC traffic consolidation. Overall, CAP strategies have shown improvement from 77% in FY 2012 to 81% in FY 2013. Progress against CAP goals is provided below in Figure 1. The previously noted metrics within larger programs have been included in the program totals. The metrics utilized in Figure 1 are:

- Continuous Monitoring: An average of: Automated Asset Management, Automated Configuration Management, and Automated Vulnerability Management;
- Strong Authentication: Comprised of PIV Logical Access (HSPD-12);
- TIC Consolidation: Comprised of TIC Traffic Consolidation;
- TIC Capabilities: Comprised of TIC 2.0 Capabilities (Includes Einstein 2); and
- Cyber CAP Progress: An average of: Continuous Monitoring, Strong Authentication, TIC Consolidation and TIC Capabilities.

Figure 1. Percentage Implementation of Administration Cyber Cross Agency Priority (CAP) Goal in FY 2012 and FY 2013



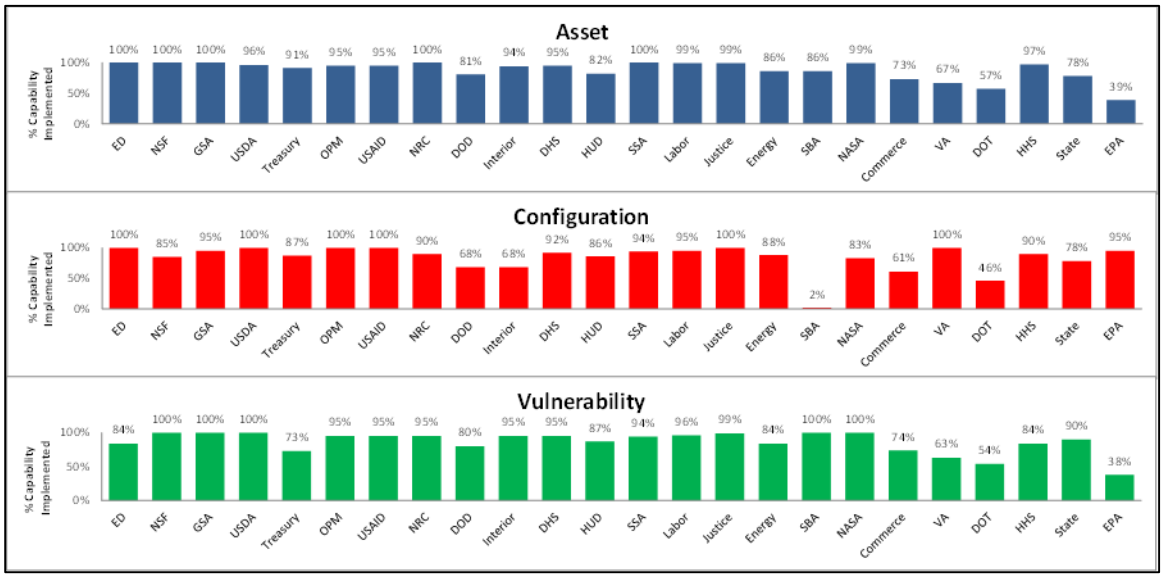
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Information Security Continuous Monitoring

As noted in Section II, ISCM is a tool for combatting information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. The continuing emphasis on adoption of ISCM will support improved security and more resilient information systems through improved situational awareness and faster remediation cycles. The Joint Continuous Monitoring Working Group, which the Executive Office of the President (EOP) has designated as the forum for interagency continuous monitoring program coordination, has determined that automated asset management, automated configuration management, and automated vulnerability management are the first areas where continuous monitoring needs to be developed. It is for this reason that these are the ISCM metrics currently being tracked.

In FY 2013, all CFO Act agencies continued to demonstrate the ability to successfully submit automated data feeds to CyberScope. Figure 2 illustrates the percentage of IT assets with automated access to asset inventory, configuration management, and vulnerability management information by agency. In FY 2013, agency implementation of automated continuous monitoring capabilities increased slightly to 81% as compared to 80% in FY 2012.

Figure 2. Percentage of Continuous Monitoring Capabilities Reported by Agencies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Although there was significant progress in the configuration management aspect of ISCM, the asset management and vulnerability management components saw slight declines. For continuous monitoring, there were more than a million additional assets reported by CFO Act agencies in FY 2013 as compared to FY 2012. Only three-quarters of these additional assets are under automated asset inventory or vulnerability management and this dropped the overall score by 3% and 2% respectively. While roughly half of the additional assets were attributable to the normal fluctuation in DOD reporting, most of the remainder were due to an increase in the scope of reporting and the installation of new asset discovery tools. This is a natural outcome of improving ISCM capabilities; as agencies focus on automation they can be expected to identify more assets. Scores will fluctuate accordingly and occasionally decline before showing steady improvement.

The goal of the ISCM asset inventory management capability is to provide a full accounting of an agency's IT assets using automation to identify and remove unmanaged assets so that those assets are under configuration management. In FY 2012, agencies reported automated inventory capturing with a success rate of 86%, but in FY 2013 the success rate decreased to 83%.

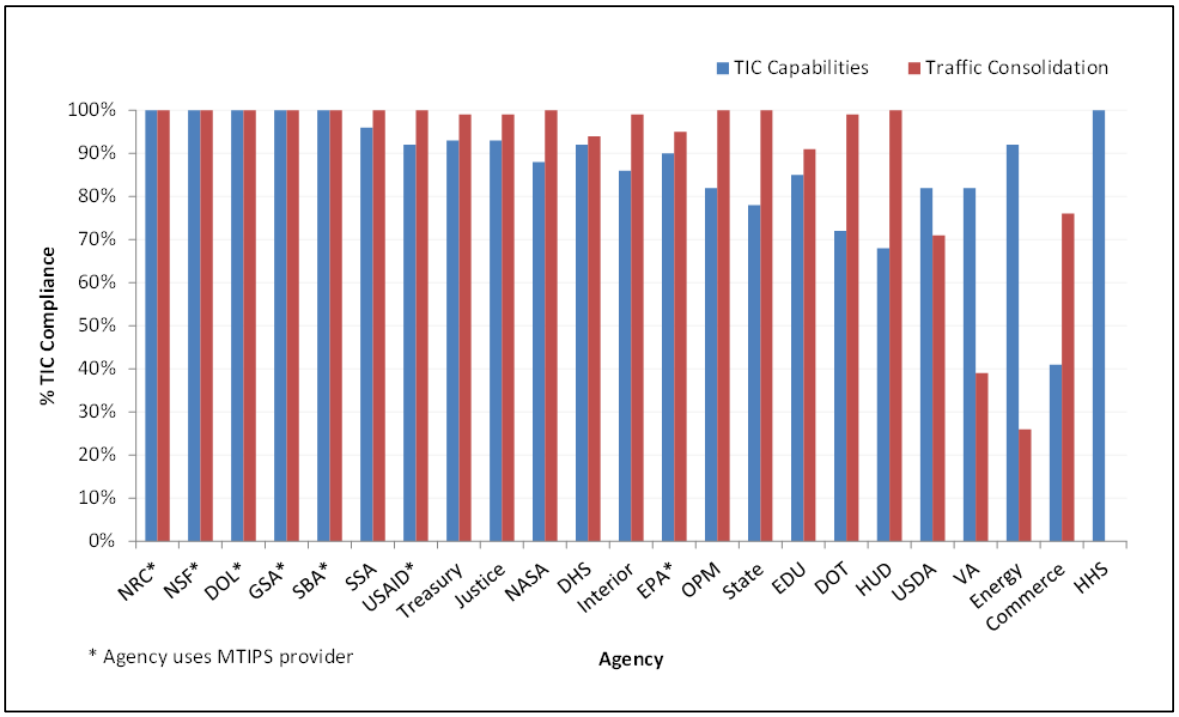
Improved configuration management and the development of secure configuration baselines allow for operating systems to be hardened, making it more difficult for attackers to exploit any vulnerability. For system configuration, automated tools were used to keep track and compare the information system baseline configurations of agencies to installed configurations in an effort to maintain consistent baselines and remediate non-compliant baseline configurations for all information systems. In FY 2012, agencies reported that the automated configuration management capability was 70%, and this level increased to 79% in FY 2013. This increase is a result of the further deployment of associated tools and sensors and more centralized reporting of data.

Agencies also made modest progress in the use of automated vulnerability management systems that scan agency IT assets for common vulnerabilities (software flaws, required patches, etc.) and facilitate remediation of those vulnerabilities to protect against intentional or unintentional misuse or malicious exploits. In FY 2012, 83% of assets were being managed with an automated vulnerability management capability. As of the end of FY 2013, analysis of the vulnerability management capability across the government shows 81% of assets are being managed with an automated vulnerability management capability.

Trusted Internet Connections (TIC)

As previously noted in Section II, the TIC initiative seeks to optimize and standardize the security of individual external network connections, including connections to the Internet. This year the initiative continued to make progress via the adoption of trusted providers for external telecommunications access points. Sixteen CFO Act agencies are TICAPS and four vendors have been designated to provide MTIPS to agencies that want the TIC capabilities but choose not to become their own TICAP. DOD implemented an equivalent initiative and thus is exempt from TIC. Agencies underwent TIC compliance validation assessments by DHS for implementation of the 60 critical security requirements that comprise the TIC Reference Architecture Version 2.0 capability. Such compliance validation was also required for the percentage of agencies' external network traffic passing through a TIC MTIPS vendor. The consolidation of external network traffic increased from 81% in FY 2012 to 86% in FY 2013 for the 24 CFO agencies (excluding DOD). The implementation of TIC Reference Architecture Version 2.0 critical security capabilities also increased from 84% in FY 2012 to 87% in FY 2013. Figure 3 illustrates percentage of TIC security capabilities and traffic consolidation as implemented by agencies.

Figure 3. Percentage of TIC Security Capabilities and Traffic Consolidation Implemented by Agencies



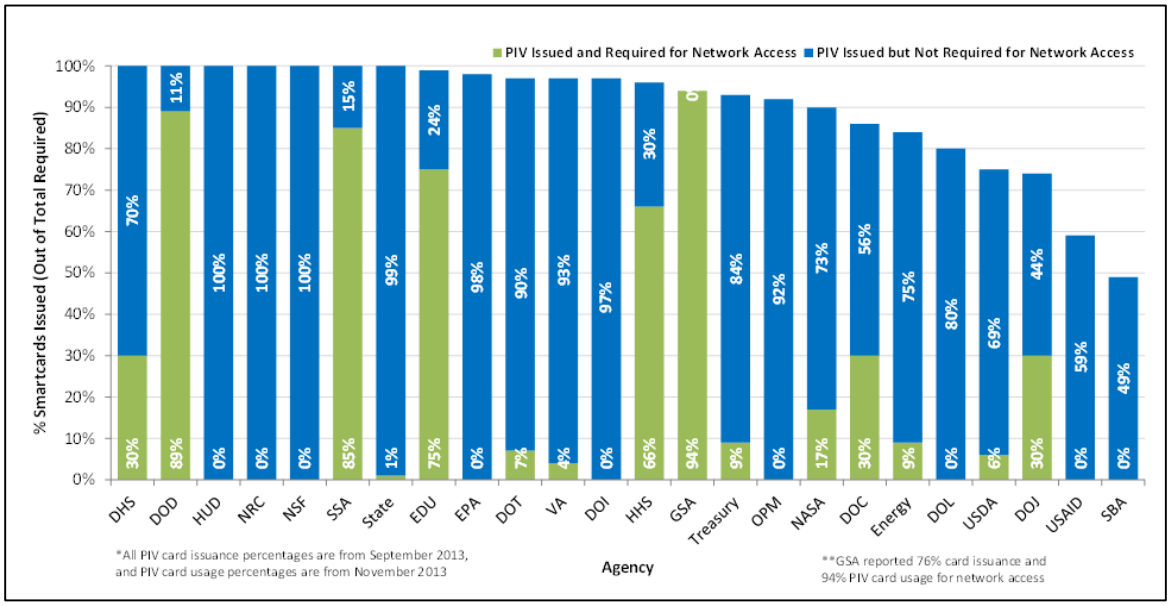
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Strong Authentication: HSPD-12

As noted in Section II, OMB issued *OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors* in February 2011, directing agencies to issue policy and formulate an action plan for the full implementation of HSPD-12. As of September 1, 2013, agencies reported that 96% of employees and contractors requiring PIV credentials (i.e., cards) have received them. With the majority of the Federal workforce now possessing the cards, agencies are in a position to accelerate the use of PIV cards for two-factor authentication to agency networks. Two-factor authentication requires two separate means of asserting an identity, such as something you have (PIV card) and something you know, such as a personal identification number (PIN), to reduce the risk of parties gaining access to government information through the use of a false identity. Figure 4 shows, by agency, the issuance progress and percentage of user accounts that require PIV cards for access to the agency's networks.

The FY 2013 FISMA metrics data indicate that 67% of government user accounts are configured to require PIV cards to authenticate to agencies' networks, up from 57% in FY 2012. Twelve of the agencies made progress in mandatory PIV use for logical access, with seven improving from 0% in FY 2012 and six showing better than 12% improvement. The Social Security Administration (SSA), Department of Justice (DOJ), DOC, HHS, and NASA made the largest improvements. At this time last year, seven agencies reported that 8% or more of user accounts required PIV cards for authentication, with four of those agencies at 45% or better. In FY 2013, mandatory PIV use increased to thirteen agencies reporting 6% or better, three agencies reporting 30%, and five agencies reporting 66% or better. Of the remaining 11 agencies, two reported between 1% and 4% of employees were required to use their PIV cards to authenticate to the agency network, and 9 reported 0%.

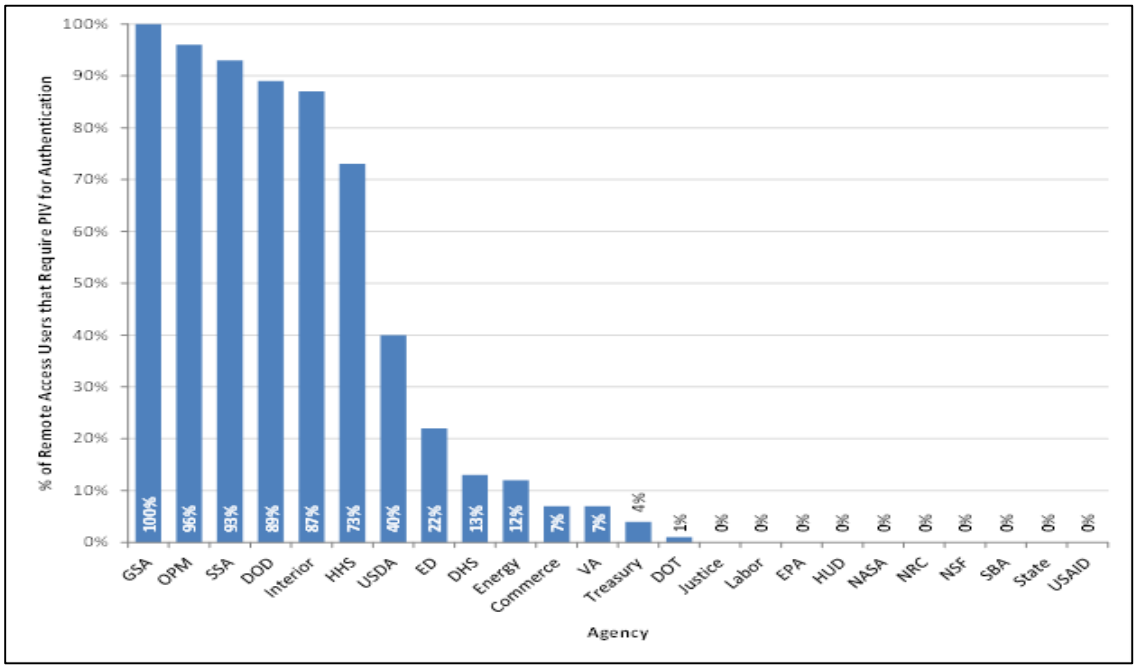
Figure 4. Smartcard Issuance Progress and Percentage of User Accounts that Require the Use of PIV Cards for Network Access Reported by Agencies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Agencies were also asked to report what percentage of people who connect to the network through remote access methods are required to use a PIV card for authentication. Across the government, 62% of remote access users were required to use a PIV card for authentication. Figure 5 shows, by agency, the percentage of user accounts that require the use of PIV cards for remote access to the agency's network.

Figure 5. Percentage of User Accounts that Require the Use of PIV Cards for Remote Network Access Reported by Agencies



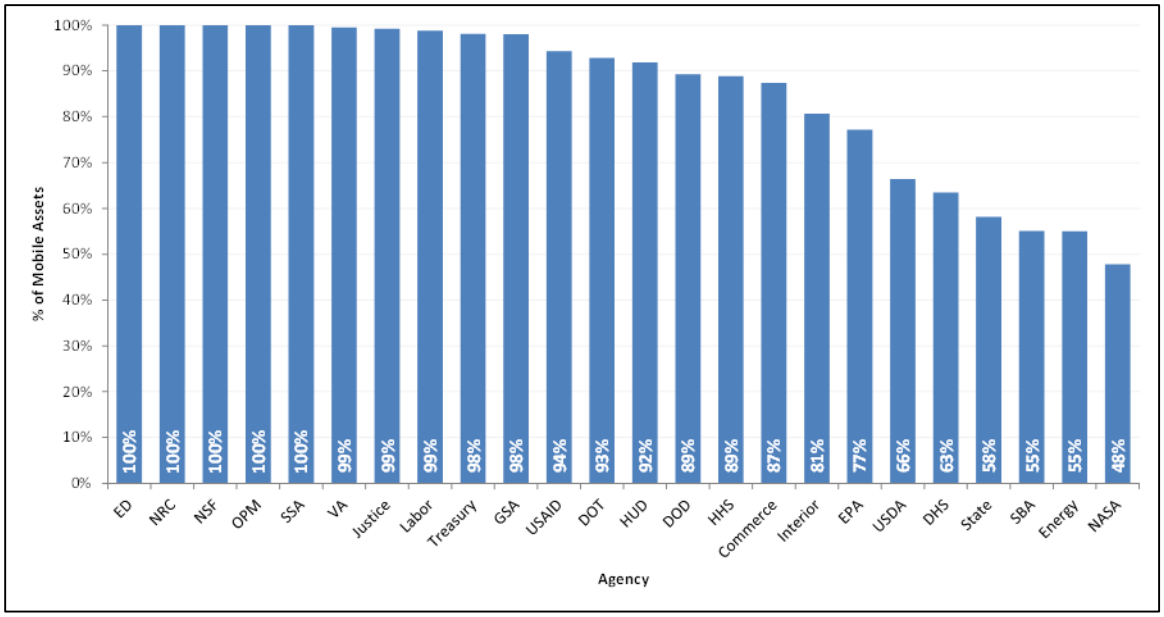
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Portable Device Encryption

As the Federal Government increasingly makes use of laptop computers and other portable computing devices, it becomes even more essential to ensure data on those devices is properly secured. It is based on this assessment that the encryption of portable devices was named an Administration priority requiring associated metrics by which to track Federal progress. The ultimate goal is to have 100% of all portable computing devices encrypted with *NIST FIPS 140-2, "Security Requirements for Cryptographic Modules,"* [xxiii] validated encryption, which specifies the security requirements for cryptographic modules utilized to protect sensitive but unclassified information, per *OMB Memorandum M-06-16, "Protection of Sensitive Agency Information."* [xxiv] Mobile devices are vulnerable to the loss of sensitive data because they move outside the protection of physical and electronic barriers that protect other hardware assets. These devices also possess unique abilities to carry malware back into the Federal Intranet environment. The encryption of data at rest and/or in motion is vital to protect data's confidentiality, integrity and/or availability. Figure 6 shows the percentage of agency portable devices with FIPS 140-2 validated encryption.

Similar to last year's metric, FY 2013 captured the encryption percentage of all mobile assets including laptops, netbooks, tablet-type computers, Blackberries, personal digital assistants, smartphones, Universal Serial Bus (USB) devices and other mobile hardware assets. In FY 2012, the reported governmentwide average was 90%, but in FY 2013 the governmentwide average declined to 84%. It should be noted that almost half a million additional mobile devices were reported in FY 2013. More than half of these additional devices were USB-connected devices, smartphones, and other cellular devices, of which less than half had encryption.

Figure 6. Percentage of Portable Devices with Encryption Reported by Agencies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Domain Name System Security Extensions (DNSSEC) Implementation and Email Validation

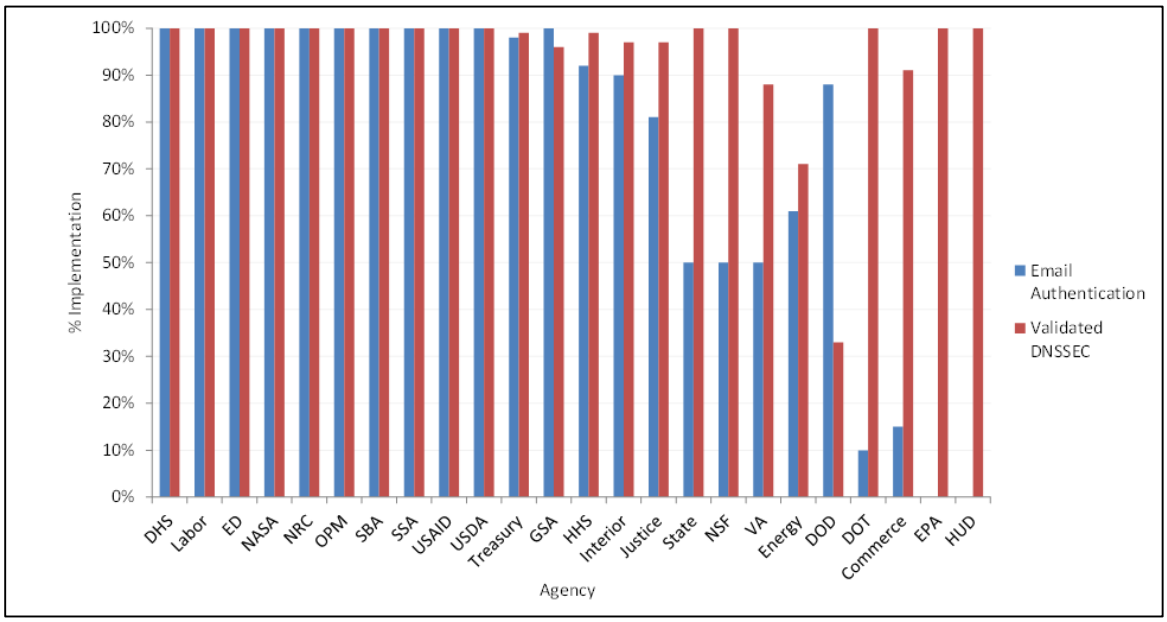
As the Government's reliance on the Internet to disseminate and provide information has increased, one of the risks it has encountered is the potential unauthorized use, compromise, and loss of the .gov domain space. As Domain Name Systems (DNS) translate website names to numeric IP addresses, attackers attempt to hijack the process to take control of the session to, for example, collect user account and password information. The key to defeating such efforts is verifying the integrity of each DNS response received. DNSSEC provides cryptographic protections to protect against such attacks by digitally 'signing' data so users can be assured it is valid, thereby mitigating the risk of DNS-based attacks and improving the overall integrity and authenticity of information processed over the Internet. The use of DNSSEC was mandated at the Federal level by *OMB Memorandum M-08-23, "Securing the Federal Government's Domain Name System Infrastructure,"* to prevent the pirating of government domain names. [xxv] GSA has ensured proper DNSSEC for the top level domain names and each organization is responsible for DNSSEC in sub-domain names, which are those below the top-level domain (i.e., www.agency.gov). The DHS Cybersecurity Assurance Program scans domains to validate the DNSSEC implementations. Fifteen agencies were validated as having 100% signed second level domains for DNSSEC:

- Department of Agriculture
- Department of Education
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of Labor
- Department of State
- Department of Transportation
- United States Agency for International Development
- Environmental Protection Administration (EPA)
- National Aeronautics and Space Administration
- National Science Foundation
- Nuclear Regulatory Commission
- Office of Personnel Management
- Small Business Administration
- Social Security Administration

Progress was reported in this capability area from FY 2012 to FY 2013, with the

governmentwide compliance rate growing from 74% in FY 2012 to 93% in FY 2013. This compliance rate is as measured by the DHS Cybersecurity Assurance Program using Cybersecurity Capability Validation (CCV) tools. DHS offers CCV tools to enable organizations to inspect for DNSSEC compliance, noting that a key reason for DNSSEC compliance problems in the past has been expiring certificates that are not updated by the owning organization. Figure 7 shows, by agency, the DNSSEC deployment and percentage of email systems with sender verification technologies.

Figure 7. Percentage of Validated DNSSEC and Email Sender Verification Reported by Agencies



Source: Data reported by DHS as measured by the DHS Cybersecurity Capability Validation (CCV) tools from October 1, 2012 to September 30, 2013

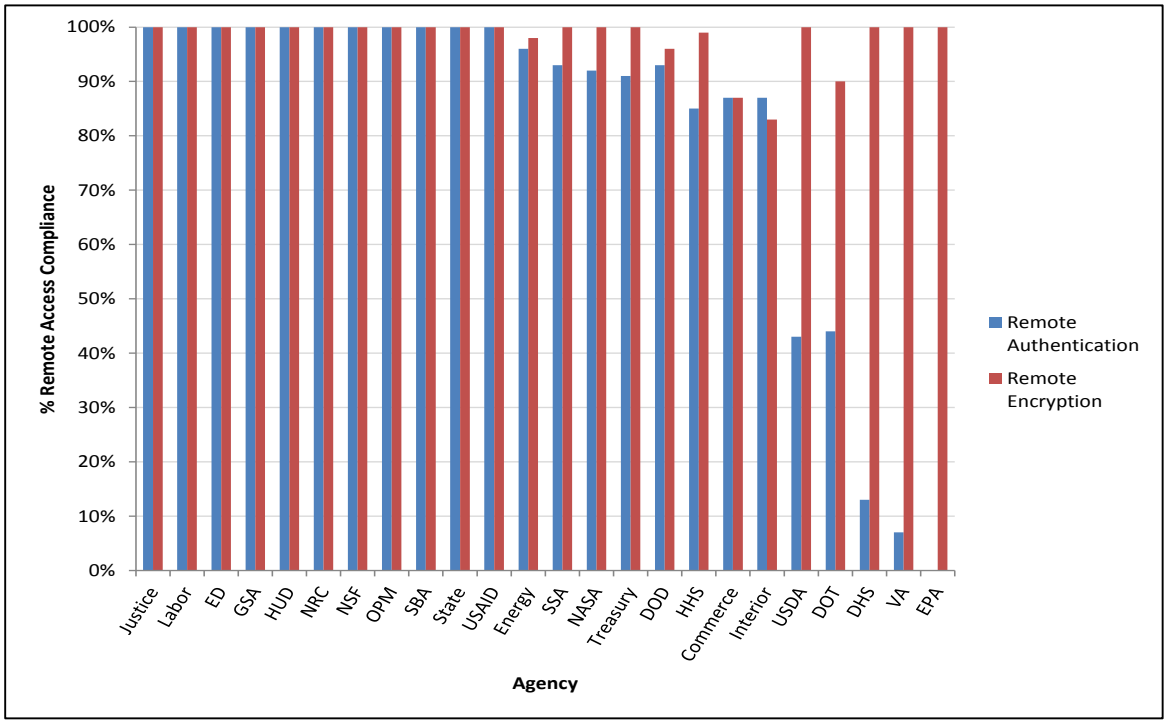
Additionally, Federal Government operations increasingly rely on email for timely and secure communication, making it essential that recipients of electronic communication from the Federal Government have assurance that the messages they receive are authentic Government correspondence. A key objective of DNSSEC is to increase the level of trust in email authenticity. However, fraudulent emails sent to Federal agencies, such as the phishing attacks described under the Security Training portion of this section as well as Section IV, also pose a significant security risk. By coupling sender verification (anti-spoofing) technologies with sender verification techniques, the security of email has been and can be further improved. In FY 2013, agencies were asked to report the percentage of agency email systems that implemented anti-spoofing technologies when sending messages and checked sender verification when receiving messages from outside the network. In FY 2012, the CFO Act agency average for email validation was reported 64%. The CFO Act agency average increased to 74% in FY 2013 with 11 agencies (just fewer than half the agencies), now achieving 100%.

Remote Access

As the Federal Government promotes telework and increases its mobile workforce, remote access to network resources must require stronger authentication mechanisms than userID and password. Agencies were asked to report their total number of agency remote access users and the percentage of those users that required only userID and password for authentication. According to FY 2013 data, almost half the agencies have totally eliminated userID and password-only methods of access, however there are still a minority of agencies that use this method for most, if not all, of their remote access connections. Across the government, 79% of remote access users were disallowed the use of userID and password combinations as a method of authentication in FY 2013. This is an increase from 53% in FY 2012, however this is partially due to a rewording of the metric in FY 2013 which provided a more accurate measure of remote authentication, focusing on users rather than connections.

Agencies were also asked how many of their remote access connections utilized FIPS 140-2 validated cryptographic modules. In FY 2012, agencies responded that 82% of their remote connections utilized such encryption. In FY 2013, remote access encryption increased to 98% of the remote connections for CFO agencies, with three-quarters of the agencies reporting 100% remote access encryption. Figure 8 shows both the percentage of remote access users, by agency, that require more than just userID and password authentication as well as remote access users requiring FIPS 140-2 encryption for connections.

Figure 8. Percentage of Remote Access Users Disallowed from Using UserID and Password for Authentication and Remote Access Users Requiring Remote Access Encryption Reported by Agencies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

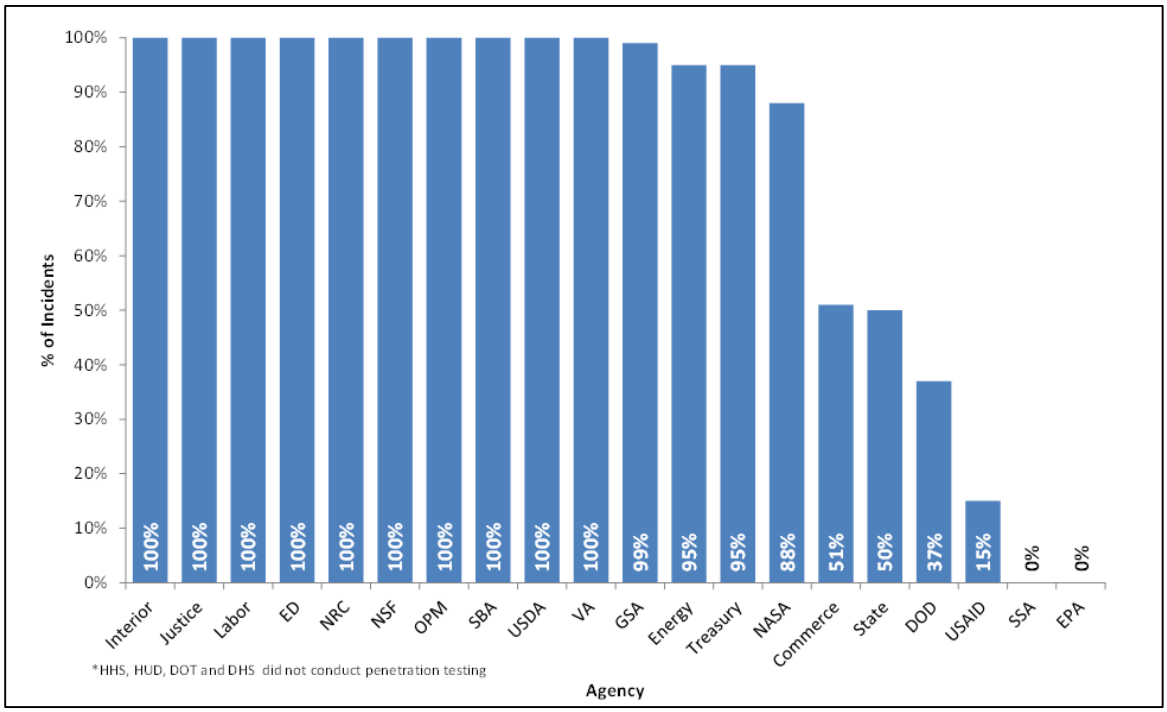
Controlled Incident Detection

Penetration testing allows organizations to test their network defenses and estimate the extent to which they are able to detect and respond to actual threats. Agencies sponsor penetration testing to determine whether defenders detect the events (pseudo-incidents) that are discovered during the controlled network penetration test. The controlled penetration testing exercises do not address actual security incidents found during routine operation of the incident management process. The intent of the exercise is to measure the detection and response capabilities of the Network Operations Center/ Security Operations Center (NOC/SOC) under simulated real-time conditions.

The results of penetration testing can be used to determine whether the NOC/SOC is staffed with the correct personnel and technologies. Although the NOC/SOC is tested in real life on a continual basis, the controlled nature of these penetration tests allows for the detection and response to be most readily measured. This also provides useful information to the risk management process to determine the level of cyber resources to invest in incident detection and response.

Across the 21 CFO Act agencies conducting controlled penetration tests, on average the NOC/SOC was 73% effective at detecting incidents, with half of the CFO Act agencies reporting a detection rate of 99% or better. This overall capability increased from 63% in FY 2012. Figure 9 illustrates the percentage of controlled penetration testing events detected by agencies.

Figure 9. Percentage of Controlled Incident Detection as Reported by Agencies



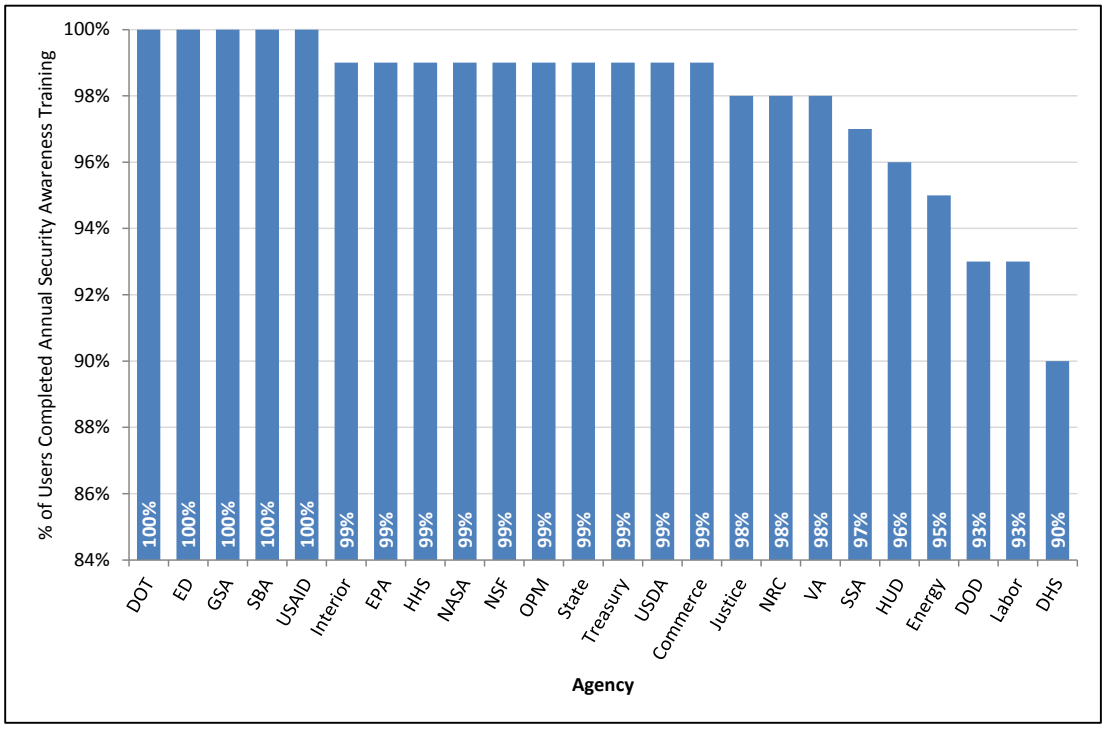
Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Security Training

Some of the most effective attacks on cyber-networks are directed at exploiting user behavior. These include phishing attacks, social engineering to obtain passwords, and introduction of malware via removable media. Phishing attacks attempt to get a network user to respond to a fraudulent message, producing a negative impact on confidentiality, integrity, and/or availability of the organization's information. These threats are especially effective when directed at those with elevated network privileges and/or other elevated cyber responsibilities. Training users, both privileged and unprivileged, as well as those with access to other pertinent information and media is a necessary deterrent to these methods. Agencies are, therefore, expected to use risk-based analysis to determine the correct amount, content, and frequency of updates in order to achieve adequate security with regards to user behavior. The FY 2013 metrics were used to assess the extent to which agencies are providing training to address these attacks and threats.

In FY 2013, more than two-thirds of the agencies sponsored emerging threat exercises (including phishing) to increase cybersecurity awareness and/or to measure the effectiveness of cybersecurity awareness training in molding behavior. Agencies are generally meeting the annual requirement for cybersecurity awareness training, with all agencies providing some form of supplemental security training during the year, and some, as a best practice, providing daily or weekly supplemental security training. For agency users with network access privileges, 94% were given annual security awareness training, which is up from 88% in FY 2012. Agencies also reported that 98% of new users were given security awareness training prior to being granted network access, up from 89% in FY 2012. Figure 10 shows, by agency, the percentage of users completing annual security awareness training.

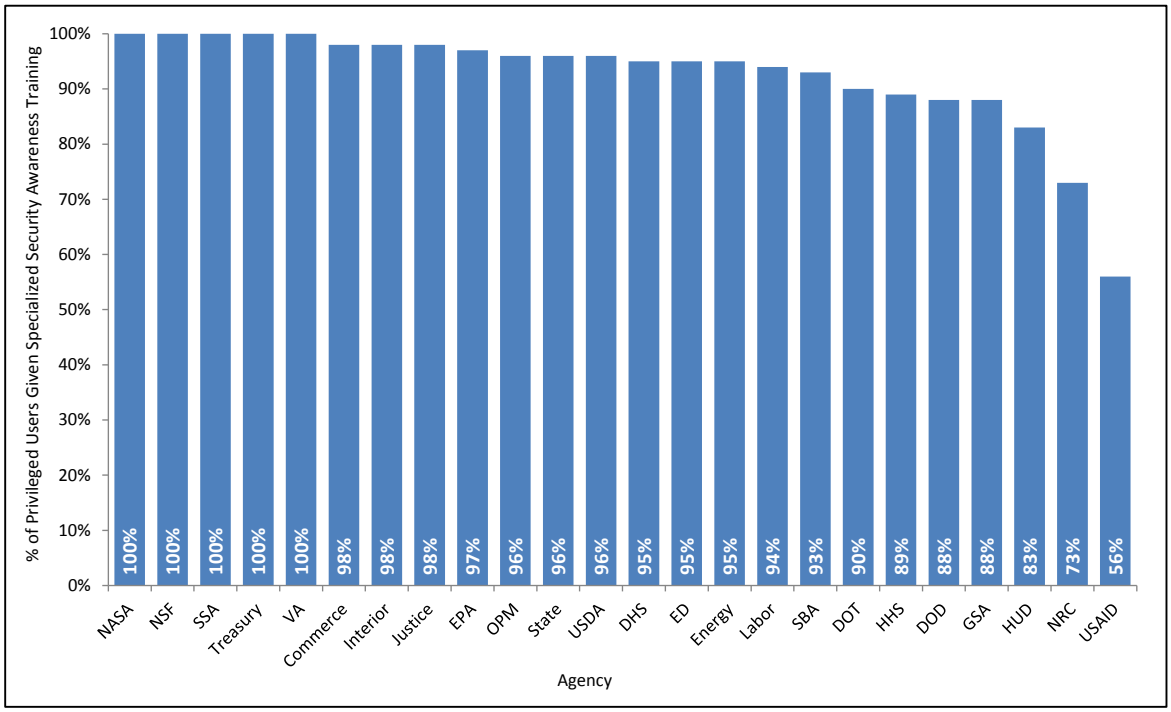
Figure 10. Percentage of Users with Network Access Completing Annual Security Awareness Training Reported by Agencies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Certain users, however, have significant security responsibilities resulting from a role where the daily assigned duties reflect an elevated level of authorized access to systems, data, and environments. This includes all users with privileged network user accounts and all other users who have managerial or operational responsibilities that allow them to increase or decrease cybersecurity. After receiving the appropriate security training, users should be able to practice good behaviors and act wisely and cautiously to increase cybersecurity and avoid behaviors that would compromise cybersecurity. These privileged users have a responsibility to ensure the protection of the elements under their purview as required by information security policies and applicable laws. Agencies were asked for the number of network users that had been given training to perform their significant cybersecurity responsibilities. Most agencies provide this training annually and specialized cybersecurity training for agency privileged users averages 92% across all CFO Act agencies in FY 2013, the same as in FY 2012. Figure 11 shows, by agency, the percentage of agency users with significant security responsibilities given specialized annual cybersecurity training.

Figure 11. Percentage of Users with Significant Security Responsibilities Given Specialized Security Training Reported by Agencies

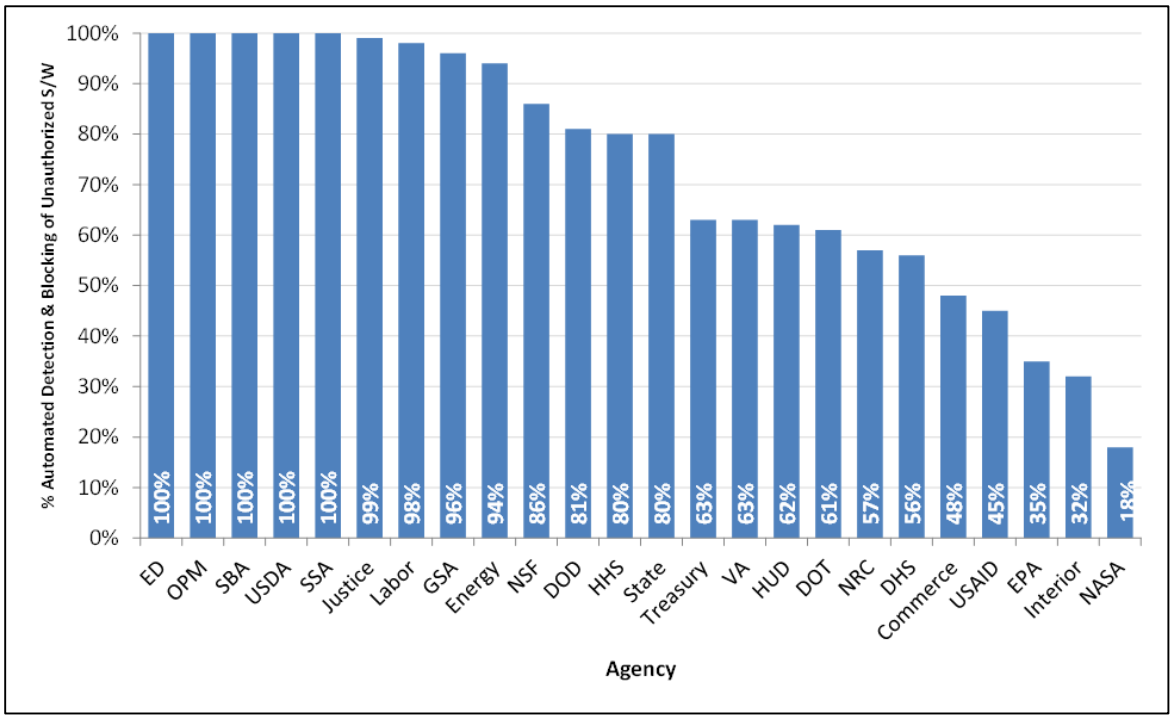


Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Automated Detection and Blocking of Unauthorized Software

Agencies were asked the number of assets for which the organization has implemented an automated capability at the device level to detect and block unauthorized software from executing. Automated capabilities could include anti-virus software (that blocks software based on signatures), other black-listing software that is of comparable breadth, or white-listing software that only allows executables with specific digital fingerprints (or comparable verification method) to execute. In other words, the software may be considered unauthorized because it is on a blacklist, or because it is not on a whitelist. Overall, agencies reported that 73% of assets were covered by this capability, an increase from the 60% reported in FY 2012, with five agencies reporting 100% of assets covered. Figure 12 shows, by agency, the percentage of assets with automated capabilities to detect and block unauthorized software from executing.

Figure 12. Percentage of Assets with Automated Capability to Detect and Block Unauthorized Software from Executing

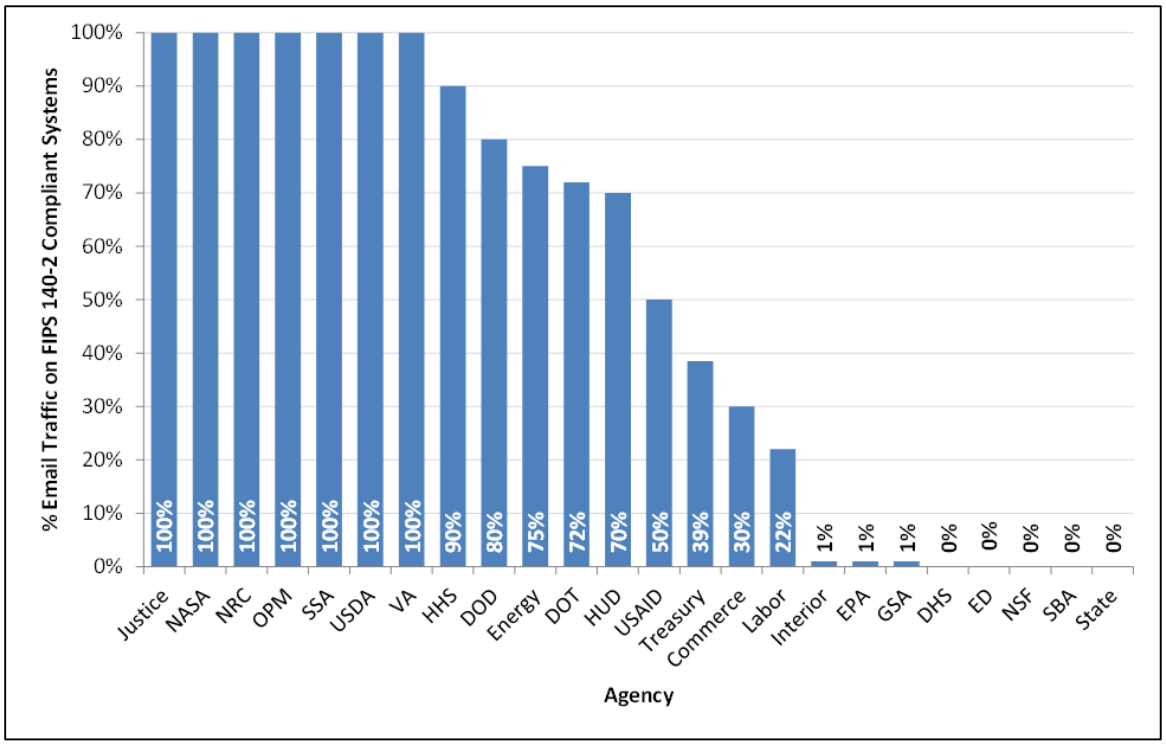


Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

Email Encryption

Unencrypted e-mails are a primary source of sensitive data loss because they move outside the protection of physical and electronic barriers that protect other hardware assets. Agencies were asked to provide the percentage of organization email traffic on systems that implement *NIST FIPS 140-2* compliant encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public, such as Secure/ Multipurpose Internet Mail Extensions (S/MIME), Pretty Good Privacy (PGP), OpenPGP, or Public Key Infrastructure (PKI). For the CFO Act agencies, 51% of email traffic occurred on systems with encryption technologies, an increase from 35% in FY 2012. Figure 13 shows, by agency, the percentage of email traffic systems that have implemented NIST FIPS 140-2 compliant encryption technologies.

Figure 13. Percentage of Email Traffic on Systems that Implement NIST FIPS 140-2 Compliant Encryption Technologies



Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013.

B. INFORMATION SECURITY METRICS FOR NON-CFO ACT AGENCIES

Background

The non-CFO Act agencies, which consist of small and micro agencies, manage a variety of Federal programs. Their responsibilities include issues concerning commerce and trade, energy and science, transportation, national security, and finance and culture. Approximately one half of all the non-CFO Act agencies perform regulatory or enforcement roles in the Executive Branch. The remaining half is comprised largely of grant-making, advisory, and uniquely chartered organizations. A "small agency" has less than six thousand employees; most have fewer than five hundred staff. A "micro agency" has fewer than 100 employees. Together these agencies employ about ninety thousand Federal workers and manage billions of taxpayer dollars. Across all non-CFO Act agencies the percentage of FISMA capabilities as reported increased from 66% to 73%.

SUMMARY OF FISCAL YEAR 2013 NON-CFO ACT AGENCIES REPORTING RESULTS

In FY 2013, 50 small and micro agencies submitted FISMA reports. The table below contains an aggregated summary of reported performance measures for those agencies that submitted reports. The small agencies responded to the exact same set of metrics in CyberScope as were presented to the CFO Act agencies, while the micro agencies reported on a subset of the FISMA metrics. Security capability areas marked with an asterisk (*) were not part of the micro agency subset of questions and the figures represent the aggregated responses from the small agencies only.

Table 2. Comparison of FISMA Capabilities from FY 2012 to FY 2013 for Non-CFO Act Agencies[1]

Capability Area	FY 2012	FY 2013
Automated Asset Management	87%	93%
Automated Configuration Management	54%	80%
Automated Vulnerability Management	65%	87%
TIC Traffic Consolidation*	62%	63%
TIC 2.0 Capabilities*	61%	60%
PIV Logical Access (HSPD-12)	3%	3%
Portable Device Encryption	84%	80%
DNSSEC Implementation*	64%	89%
E-Mail Validation Technology*	51%	71%
Remote Access Authentication	91%	90%
Remote Access Encryption*	99%	85%
Controlled Incident Detection*	53%	69%
Detect and Block Unauthorized Software*	30%	44%
User Training	85%	96%
Users with Security Responsibility Training*	95%	82%
Governmentwide Average	66%	73%

Source: Data reported to DHS via CyberScope from October 1, 2012 to September 30, 2013, except for DNSSEC data which is measured by the DHS Cybersecurity Capability Validation tools. For more information on these metrics visit: *www.dhs.gov/sites/default/files/publications/FY13%20CIO%20FISMA%20Metrics.pdf*

1 The metric for detecting and blocking unauthorized software was added to the FY13 chart to replace the US-CERT SAR metric used in the FY 2012 report.

C. INFORMATION SECURITY COST METRICS FOR CFO ACT AGENCIES

Sufficient resources must be devoted to enable the Government's information and information systems, as well as citizens' information, to remain secure. OMB requires agencies to report information security spending data on an annual basis. All CFO Act agencies reported FY 2013 spending information in the following key areas: Prevent Malicious Cyber Activity; Detect, Analyze, and Mitigate Intrusions; and Shape the Cybersecurity Environment. These areas are explained in greater detail below.

Prevent Malicious Cyber Activity

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

- TICs;
- 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:

- CERTs;
- Federal Incident Response Centers;
- Cyber threat analysis;
- Law enforcement;
- Cyber continuity of operations (COOP);
- 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:

- NSTIC;
- Workforce development;
- Employee security training;
- Standards development and propagation;
- International cooperation activities; and
- Information security and assurance research and development.

Since publishing the FY 2012 FISMA report, OMB has worked internally and with agencies to streamline and improve reporting of this spending information. Appendix 3 is the result of this coordination and presents FY 2013 information security spending for all CFO Act agencies.

SECTION IV: SECURITY INCIDENTS AND RESPONSE IN THE FEDERAL GOVERNMENT

The United States Computer Emergency Readiness Team (US-CERT) receives computer security incident reports from the Federal Government, state and local governments, commercial enterprises, U.S. citizens, and international Computer Security Incident Response Teams (CSIRTs).[2] US-CERT defines "computer security incident" as the act of violating an explicit or implied security policy.[xxvi] In accordance with Section 301 § 3544 of the E-Government Act of 2002, Federal agencies are required to notify US-CERT through the US-CERT Incident Reporting System upon the discovery of a computer security incident. The total number of computer security incidents for each group can be found in Table 3 below.

Table 3. Incidents Reported to US-CERT in FY 2013

Reporting Source	Total Number of Incidents
Federal Government Total	60,753
Federal Government: CFO Act	57,971
Federal Government: Non-CFO Act	2,782
Other (State, Local, Tribal Governments and Commercial)	158,133
TOTAL	**218,886**

Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

The total number of reported computer security incidents impacting the Federal Government increased by approximately 26% from FY 2012, while the number of reported incidents from all sectors combined increased by approximately 43% for the same period.

- In FY 2012, US-CERT received a total of 153,043 reports, of which 46,043 impacted CFO Act agencies and 2,799 impacted Non-CFO Act agencies.

- In FY 2013, US-CERT received a total of 218,886 reports, of which 60,753 impacted Federal agencies. This included both CFO Act and Non-CFO Act agencies.

Definitions for all types of computer security incidents, which are used repeatedly throughout the remainder of Section IV, are in Table 4. It should be noted that this table of definitions includes both computer security incident categories as well as selected subcategories. This is because some of the subcategories, such as phishing, represent a statistically large enough proportion of the total number of computer security incidents that OMB elected to display them separately. These distinguishable subcategories have been noted along with the larger category to which they belong.

[2] A computer security incident, as defined by NIST SP 800-61, "Computer Security Incident Handling Guide," is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

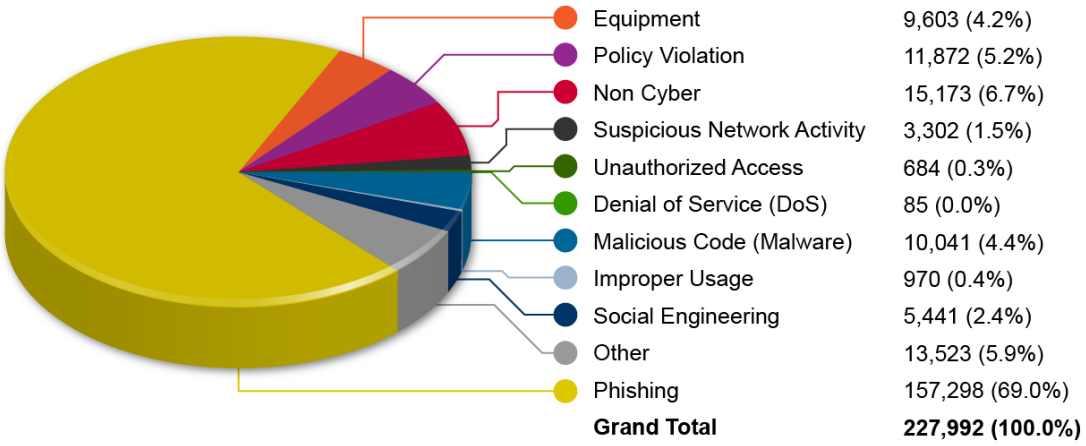
Table 4. US-CERT FY 2013 Incident Definitions

Category/Subcategories	Definition
Denial of Service (DoS)	This category is used for all successful DoS attacks, such as a flood of traffic which renders a web server unavailable to legitimate users.
Improper Usage	Improper Usage is used to categorize all incidents where a user violates acceptable computing policies or rules of behavior. These include spillage of information from one classification level to another. Policy Violation is a specific subset of this category.
-Unauthorized Access	This subset of Improper Usage 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)
-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 subset of Social Engineering, which is itself a subcategory of Unauthorized Access. (Subcategory of Unauthorized Access Subcategory)
-Phishing	This is a specific subset of Unauthorized Access / Social Engineering which is used to categorize phishing incidents and campaigns reported directly to phishing-report@us-cert.gov from both the public and private sectors. (Subcategory of Social Engineering Subcategory)
-Equipment	This subset of Unauthorized Access is used for all incidents involving lost, stolen or confiscated equipment, including mobile devices, laptops, backup disks or removable media. (Subcategory of Unauthorized Access Subcategory)
-Policy Violation	This subset of the Improper Usage Category 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 purposes of this report, a separate superset of multiple sub-categories 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 and EINSTEIN 2 data analyzed by US-CERT.

Source: Classifications and definitions provided by US-CERT

Phishing, a type of social engineering attack noted in Section II, continues to be the most widely reported incident type across total incidents reported. Figure 14 includes a breakout of all incidents reported to US-CERT in FY 2013. As Figure 14 shows, phishing accounted for 71.9% of total incidents reported, followed by non-cyber incidents at 6.9% and policy violations at 5.4%. It should be noted that Federal agencies are not required to report attempted phishing incidents and primarily report incidents that involve the actual compromise of IT assets and/or spillage of sensitive information.

Figure 14. Summary of Total Incidents Reported to US-CERT in FY 2013

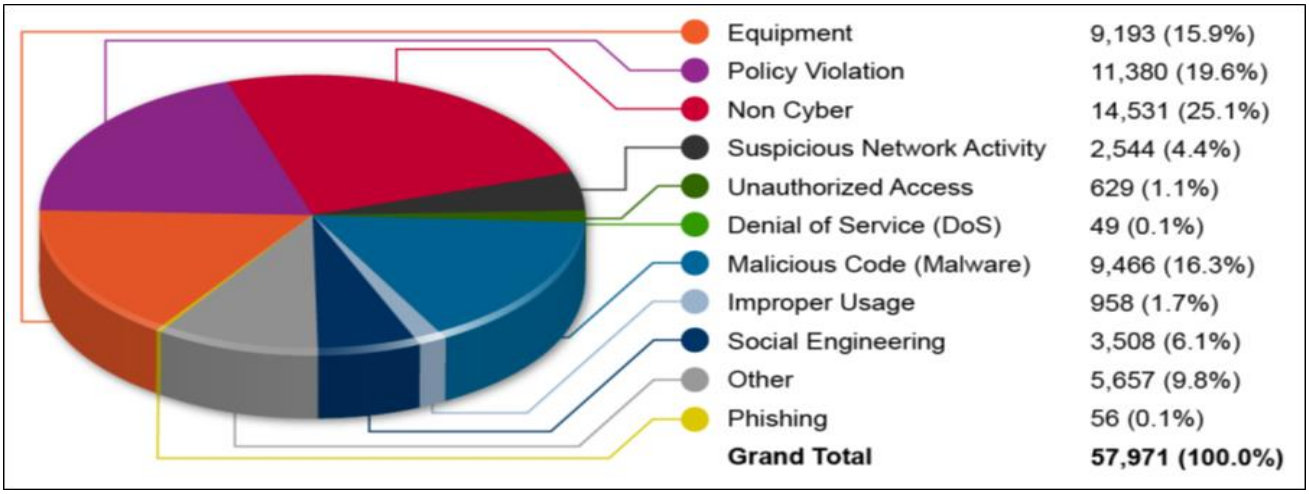


Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

CFO Act Agency Incidents Reported to US-CERT

During FY 2013, US-CERT processed 57,971 incidents reported by CFO Act agencies as shown in Figure 15. CFO Act agencies primarily reported incidents involving non-cyber incidents, which include the mishandling of sensitive information without a cybersecurity component, such as the loss of hard copy Personal Identity Information (PII) records or filing all reports of PII spillages. Policy violations also composed a substantial proportion of total incidents reported at 19.6%, as did malicious code attacks at 16.3%. A pie chart on security incidents reported by each CFO Act agency can be found in Appendix 2. A list of CFO Act agencies can be found in Appendix 5.

Figure 15. Summary of CFO Act Agency Incidents Reported to US-CERT in FY 2013

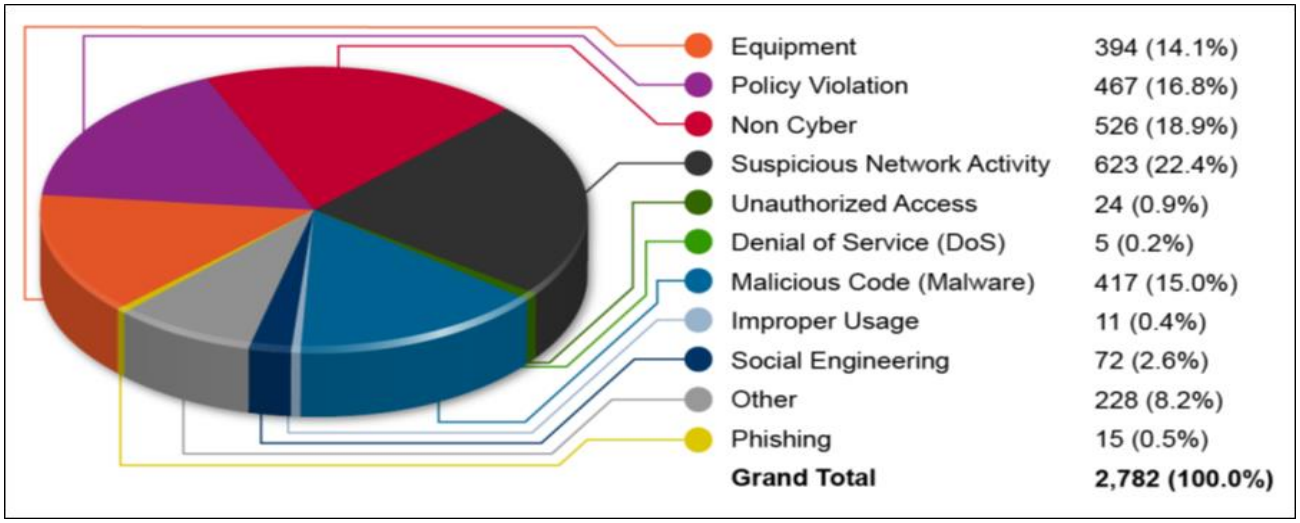


Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Non-CFO Act Agency Incidents Reported to US-CERT

During FY 2013, US-CERT processed 2,782 incidents reported by non-CFO Act agencies as catalogued in Figure 16. Non-CFO Act agencies primarily reported incidents involving infections of malicious code, policy violations, suspicious network activity and non-cyber related PII spillages. "Suspicious Network Activity" reports are indicative of suspicious, potentially unauthorized network traffic observed by US-CERT analysts utilizing the EINSTEIN sensor network. The remainder of incident reporting committed by non-CFO Act agencies is consistent in composition with CFO Act reporting, suggesting that all agencies face similar risks and deal with similar problems regardless of size.

Figure 16. Summary of Non-CFO Act Agency Incidents Reported to US-CERT in FY 2013



Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

The Federal Government continues taking significant measures to more accurately and efficiently identify and respond to security incidents when they occur. In FY 2013, US-CERT issued multiple products to Federal and private sector partners to promote information sharing and help prevent and mitigate cyber attacks. These products, which often include information gathered through analysis of suspicious network traffic detected via the EINSTEIN system, are:

- Indicator bulletins: Notifications released to agencies and partner organizations to advise of malicious activities and to provide them with indicators for administrators to prevent or identify infections in their systems;

- Analysis reports: Reports used to provide agencies with mitigation steps and enable follow up with impacted agencies; and

- Operational bulletins: Bi-weekly reports utilizing data generated through analysis of agency reporting and EINSTIEN activity to detail cybersecurity trends observed in the .gov domain.

In addition to this standard suite of products, US-CERT also engages in numerous joint efforts with the Federal Bureau of Investigation (FBI), Industrial Control Systems Computer Emergency Response Team (ICS-CERT), and the National Coordinating Center for Telecommunications (NCC), among other organizations. US-CERT's collaboration with the

aforementioned entities has generated new lines of products such as the Joint Indicator Bulletin and the Joint Analysis Report.

The Federal Government also continues to sponsor research and development of an insider threat assessment methodology and corresponding mitigation strategies through the *CERT Insider Threat Center*, a federally funded research and development center at Carnegie Mellon University's Software Engineering Institute. This effort allows for ongoing case collection and analysis, development of a scalable, repeatable insider threat vulnerability assessment method, creation of a training and certification program, and development of new insider threat controls in the CERT Insider Threat Lab. Mitigating the malicious insider remains a significant challenge and requires the composite application of several tactics and capabilities. The CERT Insider Threat Center has accelerated, and will facilitate, the identification and adoption of future insider threat controls through FISMA.

SECTION V: SUMMARY OF INSPECTORS GENERAL'S FINDINGS

Each agency Inspector General (IG) was asked to assess his or her department's information security programs in the following areas:

- Continuous monitoring management;
- 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;
- Contractor systems; and
- Security capital planning.

The IGs were asked to evaluate 99 attributes across these areas and determine whether their agencies established a program for information security in each area. The IGs were then asked to determine whether specific elements were in place for each program. Amongst both the CFO Act agencies and the small and micro agencies, the strongest areas were incident response and reporting, security training, plans of action and milestones, and remote access, while the weakest performances occurred in continuous monitoring management, configuration management, risk management, and contingency planning.

CFO Act Agencies

Table 5 summarizes the results from the IGs of the 24 CFO Act agencies according to cyber security program area. These results indicate that the departments performed best in incident response and reporting, security training, remote access management, and security capital planning. The weakest performances occurred in information security continuous monitoring management, configuration management, risk management and contingency planning.

Table 5. Results for CFO Act agencies by Cyber Security Area

Cyber Security Program Area	Program in place		Program not in place	
	FY 2013	%	FY 2013	%
Information security continuous monitoring	17	74	6	26
Configuration management	15	63	8	35
Identity and access management	18	78	5	22
Incident response and reporting	22	96	1	4
Risk management	17	74	6	26
Security training	21	91	2	9
POA&M	20	87	3	13
Remote access management	22	96	1	9
Contingency planning	18	78	5	22
Contractor systems	17	74	6	26
Security capital planning	21	91	2	9

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

Table 6 shows the CFO Act agencies' compliance scores for FY 2013 and FY 2012. The table is organized according to agencies' FY 2013 compliance scores. Ten large agencies had programs in place for all eleven areas, although each identified areas for improvement. The other 13 agencies had at least one area for which it did not have a program. The numbers of areas with deficiencies were used to compute compliance scores. Six agencies scored over 90% compliance, 11 scored between 65 and 90% compliance, and the remaining 6 scored less than 65%. Due to difference between general FISMA metric requirements and DOD program specifications, the DOD OIG requested DOD's score be displayed as "N/A". The average score was 76% for both fiscal years 2013 and 2012, respectively – no significant change.

Table 6. CFO Act agencies' Compliance Scores

Agency	FY 2013 (%)	FY 2012 (%)
Department of Homeland Security	99	99
General Services Administration	98	99
Department of Justice	98	94
Nuclear Regulatory Commission	98	99
Social Security Administration	96	98
National Aeronautics and Space Administration	91	92
Department of Education	89	79

Agency	FY 2013 (%)	FY 2012 (%)
National Science Foundation	88	90
Department of Commerce[3]	87	61
United States Agency for International Development (USAID)	83	66
Office of Personnel Management	83	77
Department of Veterans Affairs	81	81
Department of the Interior	79	92
Environmental Protection Agency	77	77
Department of Labor	76	82
Department of the Treasury	76	76
Department of Energy	75	72
Department of Transportation	61	53
Small Business Administration	55	57
Department of State	51	53
Department of Health and Human Services	43	50
U.S. Department of Agriculture	37	34
Department of Housing and Urban Development	29	66
Department of Defense[4]	N/A	N/A

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

[3] DOC OIG performed a risk assessment and focused its review on a limited number of attributes. The scoring is based on a modified methodology to reflect this.

[4] Due to difference between general FISMA metric requirements and DOD program specifications, the DOD OIG has requested DOD's score be displayed as "N/A".

Small and Micro Agencies

The results for the small and micro agencies were comparable to those of the 24 CFO Act agencies. Table 7 summarizes the results from the IGs of the small and micro agencies according to cyber security program area. These results indicate that the departments performed best in incident response and reporting, security training, plans of action and milestones, and remote access management. The weakest performances occurred in continuous monitoring management, configuration management, identity and access management, risk management, contingency planning, contractor systems, and security capital planning.

Table 7. Results for Micro Agencies by Cyber Security Area

Cyber Security Program Area	Program in place		Program not in place	
	FY 2013	%	FY 2013	%
Continuous monitoring	22	58	16	42
Configuration management	23	61	15	39
Identity and access management	28	74	10	26
Incident response and reporting	31	82	7	18
Risk management	24	63	14	37
Security training	29	76	9	24
POA&M	29	76	9	24
Remote access management	29	76	9	24
Contingency planning	26	68	12	32
Contractor systems	28	74	10	26
Security capital planning	25	66	13	34

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

Table 8 provides the small and micro agencies' compliance scores for FY 2013. The Federal Retirement Thrift Investment Board, Federal Election Commission, and Office of Special Counsel did not provide sufficient information for scoring in FY 2013. Thirteen small and micro agencies had programs in place for all eleven areas, although, like the CFO Act agencies in the same situation, each identified areas for improvement. The other 25 agencies had at least one area for which it did not have a program. The numbers of areas with deficiencies were used to compute compliance scores. Eight agencies scored over 90% compliance, 20 scored between 65 and 90% compliance, and the remaining 10 scored less than 65%. The average score was 70% for fiscal years 2013, which is comparable to the CFO Act agencies.

Table 8. Micro Agencies' Compliance Scores

Agency[5]	FY 2013 (%)
Equal Employment Opportunity Commission	99%
Tennessee Valley Authority	99%
Farm Credit Administration	99%

[5] Federal Retirement Thrift Investment Board, Federal Election Commission, and Office of Special Counsel did not provide the answers with the detail required for scoring for FY 2013.

Agency[5]	FY 2013 (%)
Federal Energy Regulatory Commission	99%
Export-Import Bank of the United States	96%
Federal Housing Finance Agency	95%
Federal Trade Commission	92%
National Endowment for the Arts	92%
Merit Systems Protection Board	88%
Smithsonian Institution	88%
Federal Reserve Board	88%
National Labor Relations Board	87%
National Endowment for the Humanities	87%
Federal Deposit Insurance Corporation	87%
Federal Labor Relations Authority	84%
Millennium Challenge Corporation	84%
Other Defense Civil Programs	84%
National Credit Union Administration	83%
Commodity Futures Trading Commission	81%
Railroad Retirement Board	80%
Securities and Exchange Commission	80%
National Transportation Safety Board	78%
Overseas Private Investment Corporation	74%
Corporation for National and Community Service	72%
Consumer Financial Protection Bureau	72%
Pension Benefit Guaranty Corporation	71%
Court Services and Offender Supervision Agency	71%
Federal Mediation and Conciliation Service	65%
Federal Maritime Commission	54%
International Boundary and Water Commission	53%
International Trade Commission	51%
Broadcasting Board of Governors	50%
Peace Corps	33%
Consumer Product Safety Commission	30%
National Archives and Records Administration	18%
Federal Retirement Thrift Investment Board	N/A
Federal Election Commission	N/A
Office of Special Counsel	N/A

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

SECTION VI: PROGRESS IN MEETING KEY PRIVACY PERFORMANCE MEASURES

Protecting individual privacy remains a top Administration priority. The importance of fully protecting privacy has become even greater as Federal agencies continue to use emerging technologies such as cloud computing, mobile computing devices and services, and social media. Federal agencies must take steps to analyze and address privacy issues at the earliest stages of the planning process, and they must continue to manage information responsibly throughout the life cycle of the information.

In addition, Federal agencies are expected to demonstrate continued progress in all aspects of privacy protection and to ensure compliance with all privacy requirements in law, regulation, and policy. 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. Agencies must work with their Senior Agency Official for Privacy (SAOP) to ensure that all privacy impact assessments (PIAs) and system of records notices (SORNs) are completed and up to date. Finally, agencies must continue to implement appropriate data breach response procedures and update those procedures as needed.

As shown in Table 9 and discussed in this section, the FY 2013 agency FISMA reports indicate improvements have been made in many privacy performance measures.

Table 9. Status and Progress of Key Privacy Performance Measures

	FY 2011	FY 2012	FY 2013
Number of systems containing information in identifiable form	4,282	4,941	4,395
Number of systems requiring a Privacy Impact Assessment (PIA)	2,600	2,778	2,586
Number of systems with a PIA	2,414	2,612	2,436
Percentage of systems with a PIA	93%	94%	94%
Number of systems requiring a System of Records Notice (SORN)	3,366	3,498	3,343
Number of systems with a SORN	3,251	3,339	3,196
Percentage of systems with a SORN	97%	95%	96%

Source: Data reported to DHS via CyberScope and provided to the Office of Information and Regulatory Affairs (OIRA) from October 1, 2012, to September 30, 2013.

Privacy Program Oversight

In FY 2013, 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 agency reported SAOP participation in two out of the three categories. In

addition, all 24 CFO Act agencies reported having policies in place to ensure that all personnel with access to Federal data are familiar with information privacy requirements and that employees who need it receive targeted, job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 100% of applicable systems to be covered by PIAs. In FY 2013, 94% of applicable systems across the 24 CFO Act agencies had up-to-date PIAs covering applicable systems. Agencies were able to maintain the improvement that was made in FY 2012.

Written Policies for Privacy Impact Assessments and Web Privacy Practices

In FY 2013, all 24 CFO Act agencies reported having written policies in place for the following topics:

- Determining whether a PIA is needed;
- Conducting a PIA;
- Evaluating changes in technology or business practices that are identified during the PIA process;
- Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA;
- Making PIAs available to the public as required by law and OMB policy;
- Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained;
- Making appropriate updates and ensuring continued compliance with stated web privacy policies.
- Monitoring the agency's systems and practices to determine when and how PIAs should be updated; and
- Determining circumstances where the agency's web-based activities warrant additional consideration of privacy implications.

In addition, 22 out of 24 CFO Act agencies agencies reported having written policies in place for requiring machine readability of public-facing agency websites.

System of Records Notices

The goal for the Federal Government is for 100% of applicable information systems that include records subject to the Privacy Act of 1974 to be covered by a published, up-to-date SORN. In FY 2013, 96% of information systems across government with records subject to the Privacy Act have published corresponding SORNs. This reflects a 1% increase in compliance from FY 2012.

Agency Use of Web Management and Customization Technologies

In FY 2013, 23 out of 24 CFO Act agencies reported use of web management and customization technologies. All 23 of those agencies reported having procedures for annual review, continued justification and approval, and public notice of their use of web management and customization technologies.

SECTION VII: APPENDICES

APPENDIX 1: NIST PERFORMANCE IN FY 2013

Section 301, §3543 of the E-Government Act of 2002 requires "an assessment of the development, promulgation, adoption of, and compliance with standards developed under Section 20 of the National Institute of Standards and Technology Act." Since the passage of the E-Government Act of 2002, NIST has worked to comply with FISMA requirements detailed in Section 303 of the Act. This includes developing and updating standards, and guidelines for information systems used or operated by Federal agencies, providing agencies with technical assistance as requested, conducting research to determine the extent of information security vulnerabilities, developing and revising performance indicators, and evaluating security policies and practices.

The activities conducted by NIST in accordance with the Act are ongoing. For a comprehensive list of activities completed by NIST in FY 2013 as required by the Act, please see NIST's website at: *www.csrc.nist.gov/about/index.html.* Additionally, as required by Section 303, NIST prepares an annual report on activities undertaken in the previous year. A copy of the most recent NIST Computer Security Division Annual Report is available online at: *www.csrc.nist.gov/publications/PubsTC.html*.

APPENDIX 2: SECURITY INCIDENTS BY CFO ACT AGENCY

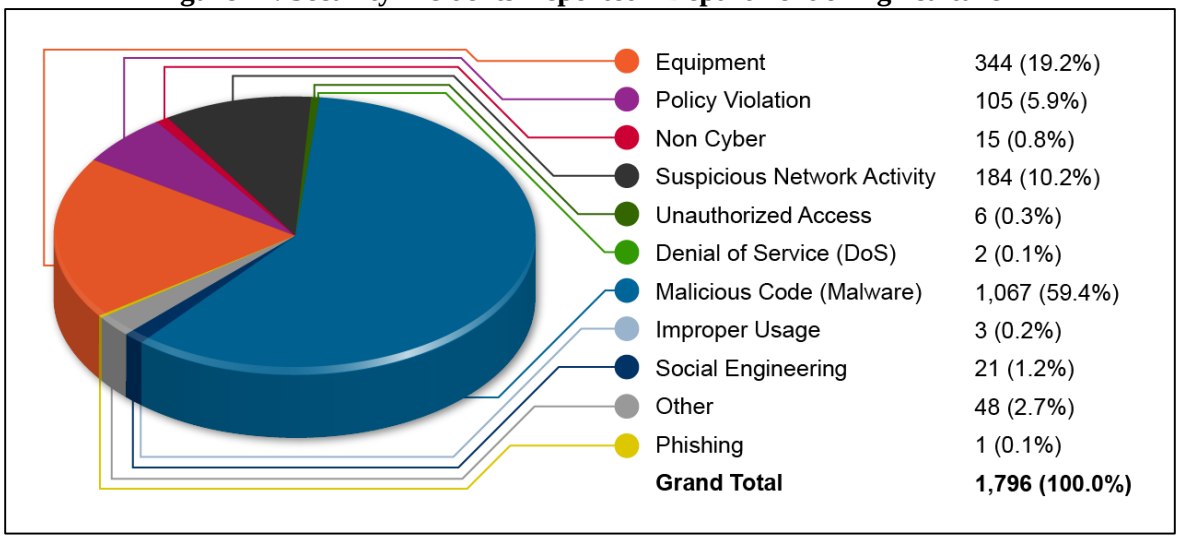
The charts in this appendix illustrate a breakdown of the types of security incidents reported by each CFO Act Agency. The definitions that are used are the same as those utilized in Section IV, however they have been relisted here for ease of access.

Table 10. US-CERT FY 2013 Incident Definitions

Category/Subcategories	Definition
Denial of Service (DoS)	This category is used for all successful DoS attacks, such as a flood of traffic which renders a web server unavailable to legitimate users.
Improper Usage	Improper Usage is used to categorize all incidents where a user violates acceptable computing policies or rules of behavior. These include spillage of information from one classification level to another. Policy Violation is a specific subset of this category.
-Unauthorized Access	This subset of Improper Usage 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)
-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 subset of Social Engineering, which is itself a subcategory of Unauthorized Access. (Subcategory of Unauthorized Access Subcategory)
-Phishing	This is a specific subset of Unauthorized Access / Social Engineering which is used to categorize phishing incidents and campaigns reported directly to phishing-report@us-cert.gov from both the public and private sectors. (Subcategory of Social Engineering Subcategory)
-Equipment	This subset of Unauthorized Access is used for all incidents involving lost, stolen or confiscated equipment, including mobile devices, laptops, backup disks or removable media. (Subcategory of Unauthorized Access Subcategory)
-Policy Violation	This subset of the Improper Usage Category 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 purposes of this report, a separate superset of multiple sub-categories 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 and EINSTEIN 2 data analyzed by US-CERT.

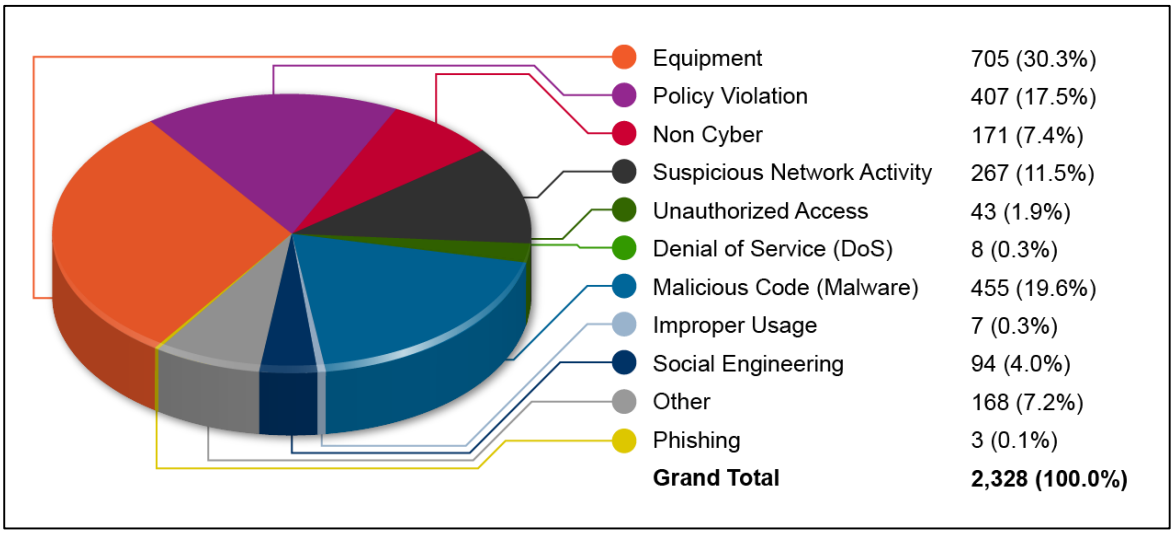
Source: Classifications and definitions provided by US-CERT

Figure 17. Security Incidents Reported - Department of Agriculture



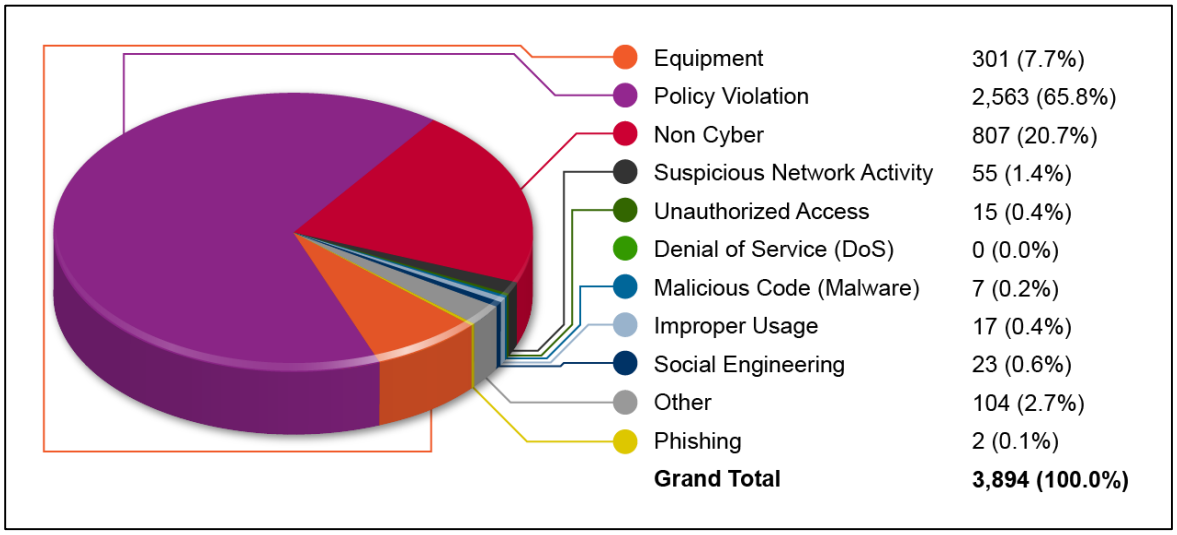
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 18. Security Incidents Reported - Department of Commerce



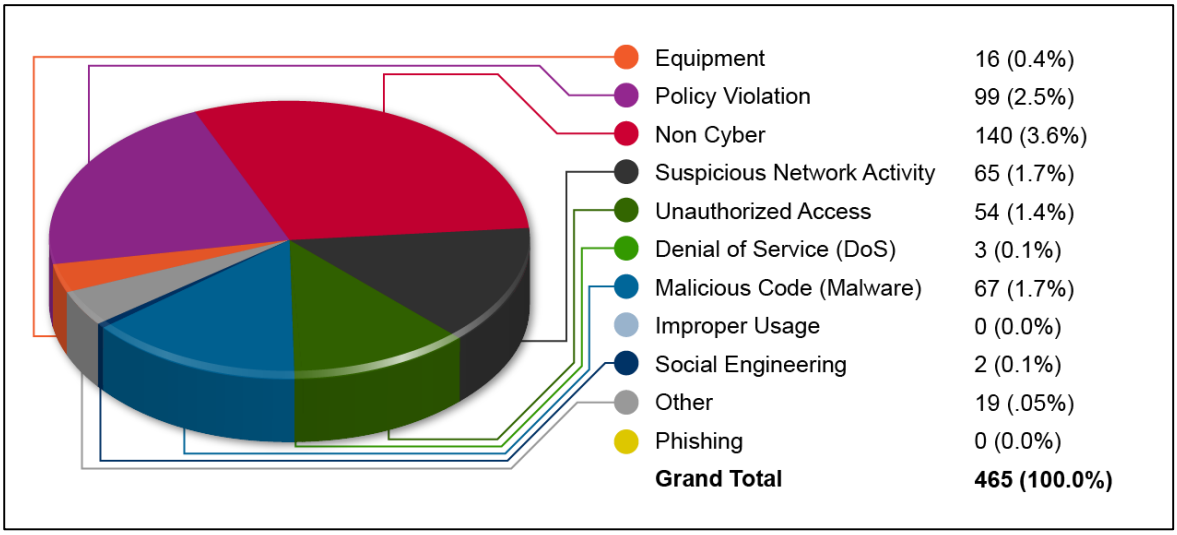
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 19. Security Incidents Reported - Department of Defense



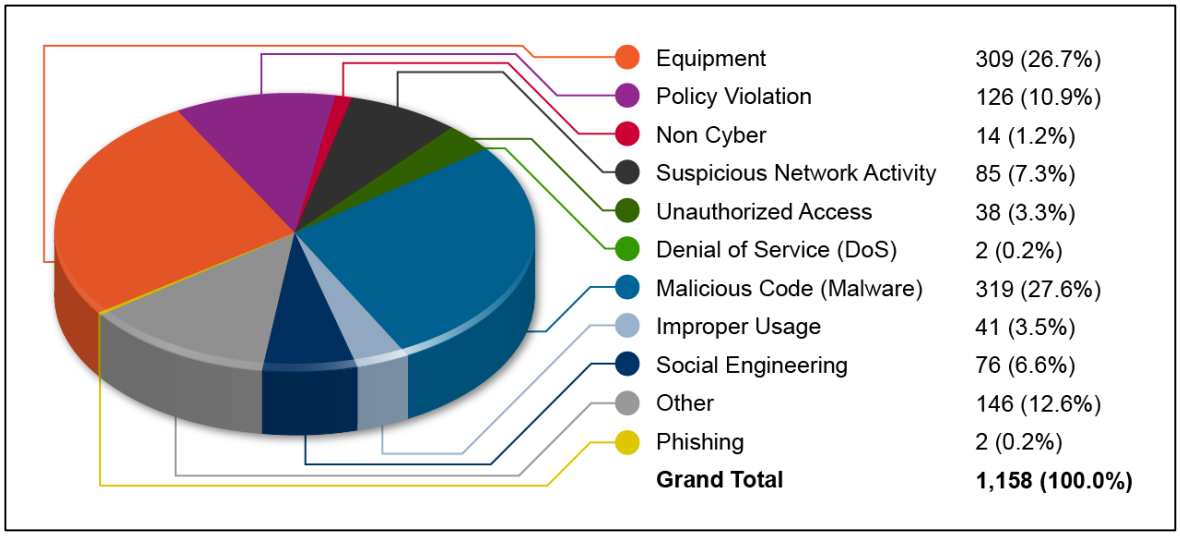
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 20. Security Incidents Reported - Department of Education



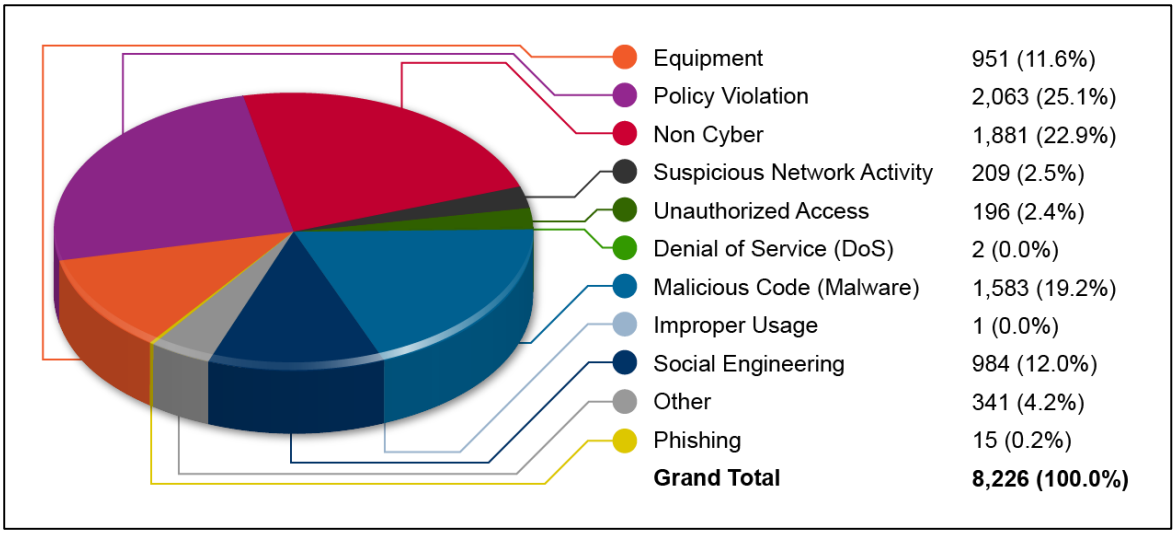
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 21. Security Incidents Reported - Department of Energy



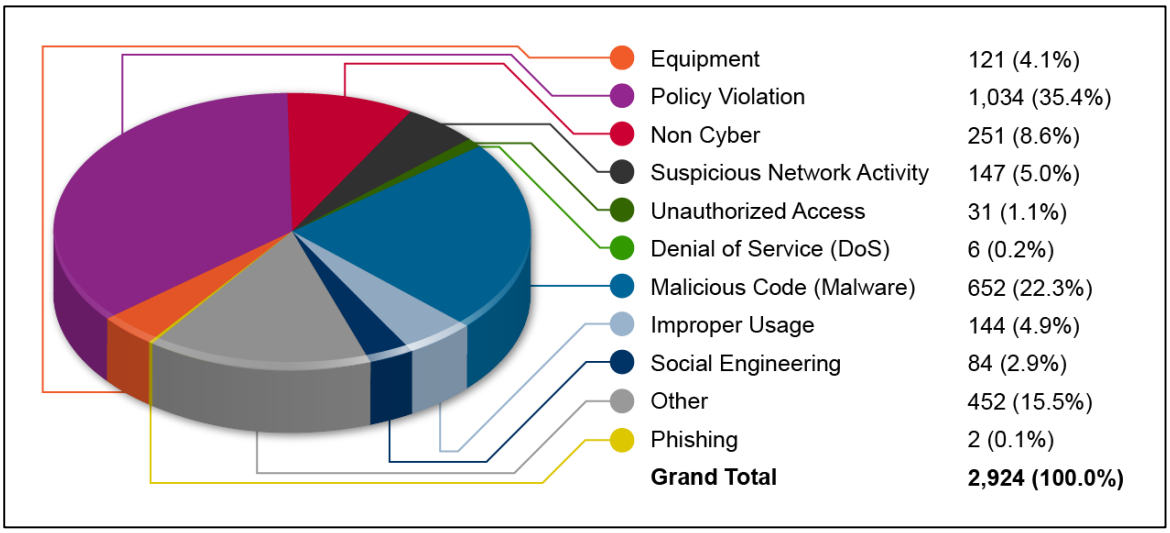
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 22. Security Incidents Reported - Department of Health and Human Services



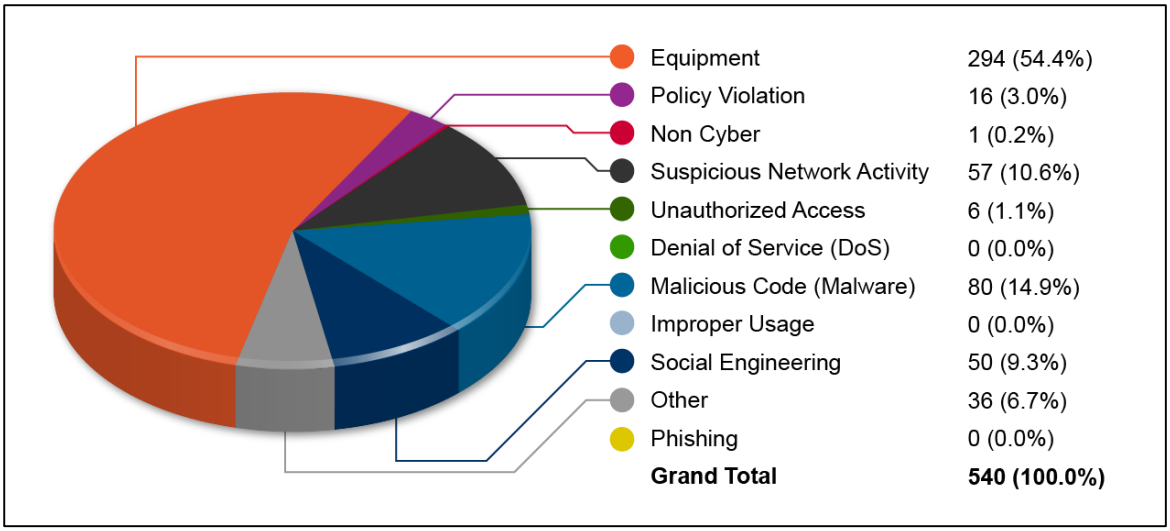
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 23. Security Incidents Reported - Department of Homeland Security



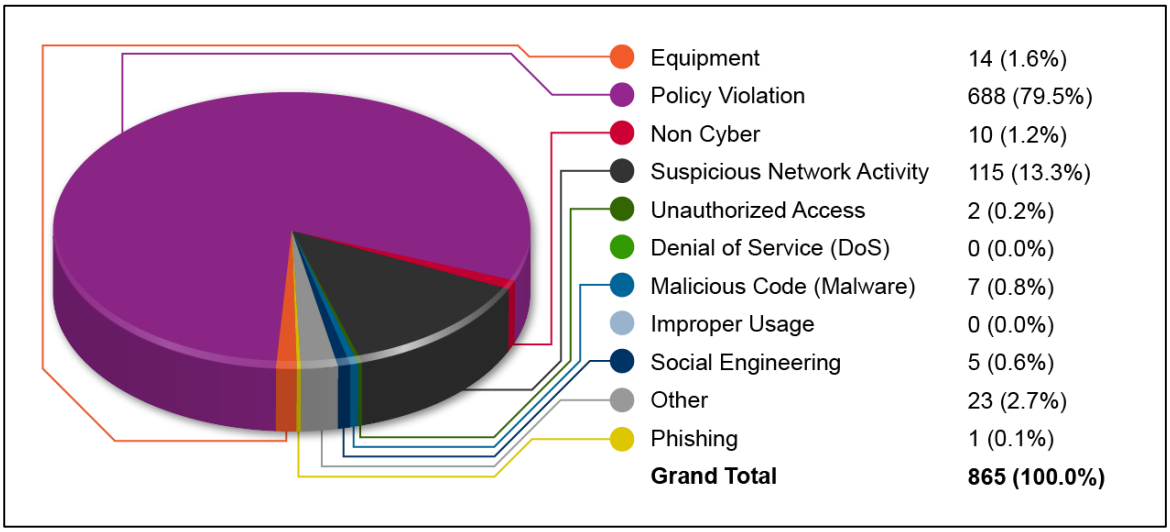
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 24. Security Incidents Reported - Department of Housing and Urban Development



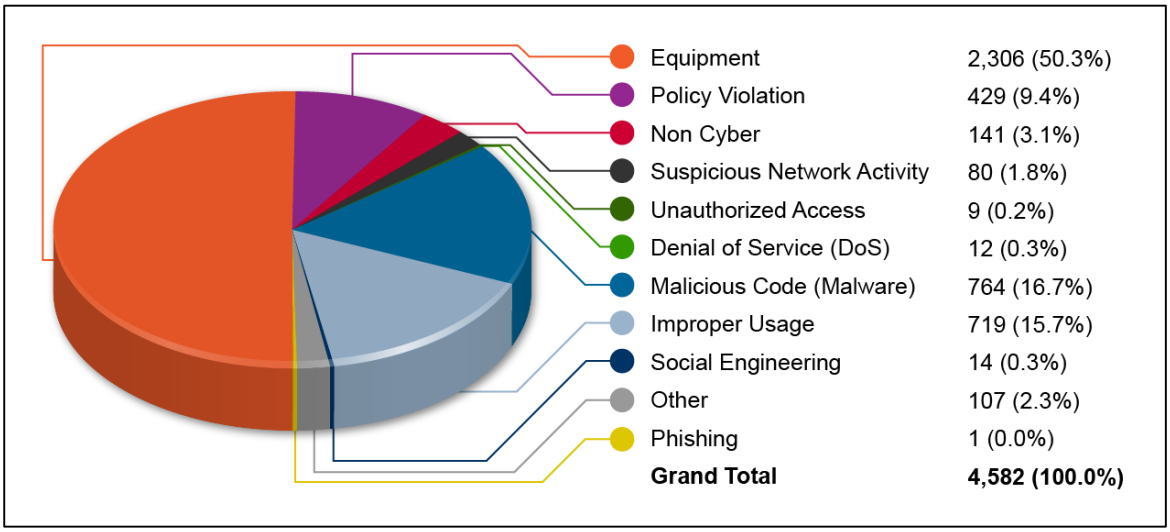
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 25. Security Incidents Reported - Department of the Interior



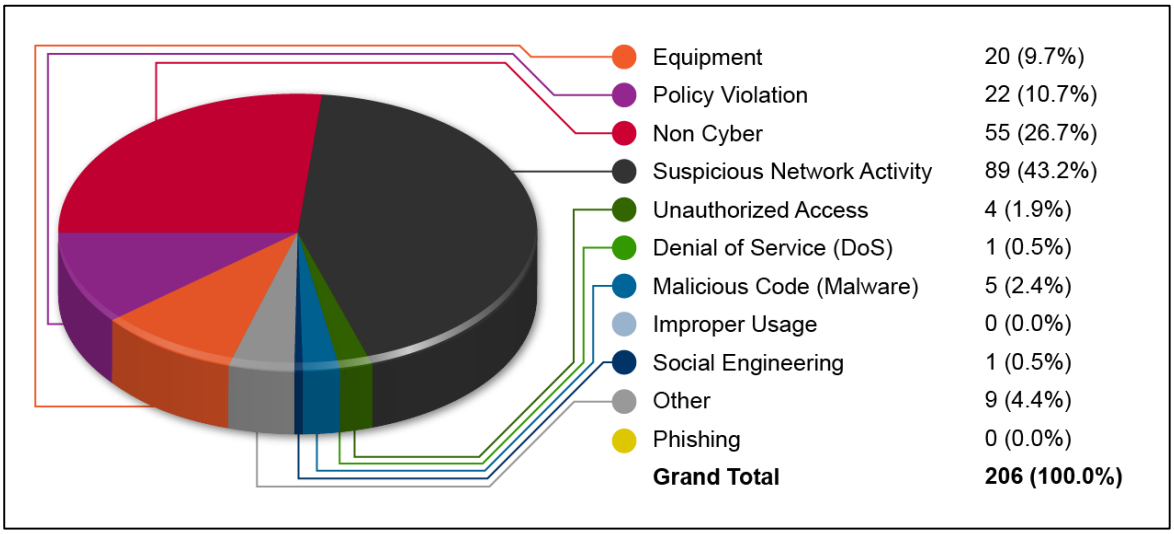
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 26. Security Incidents Reported - Department of Justice



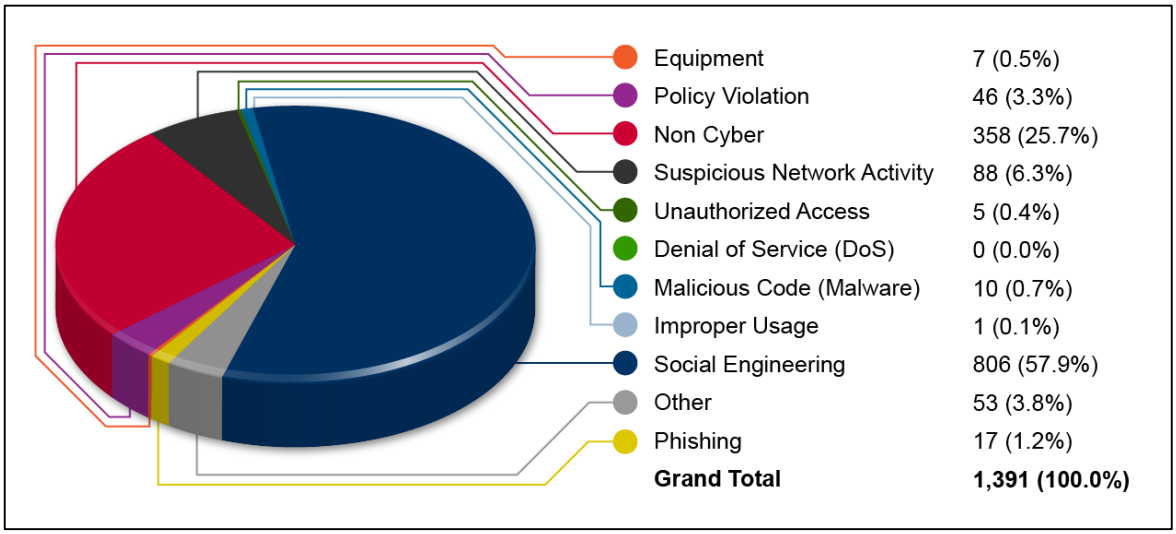
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 27. Security Incidents Reported - Department of Labor



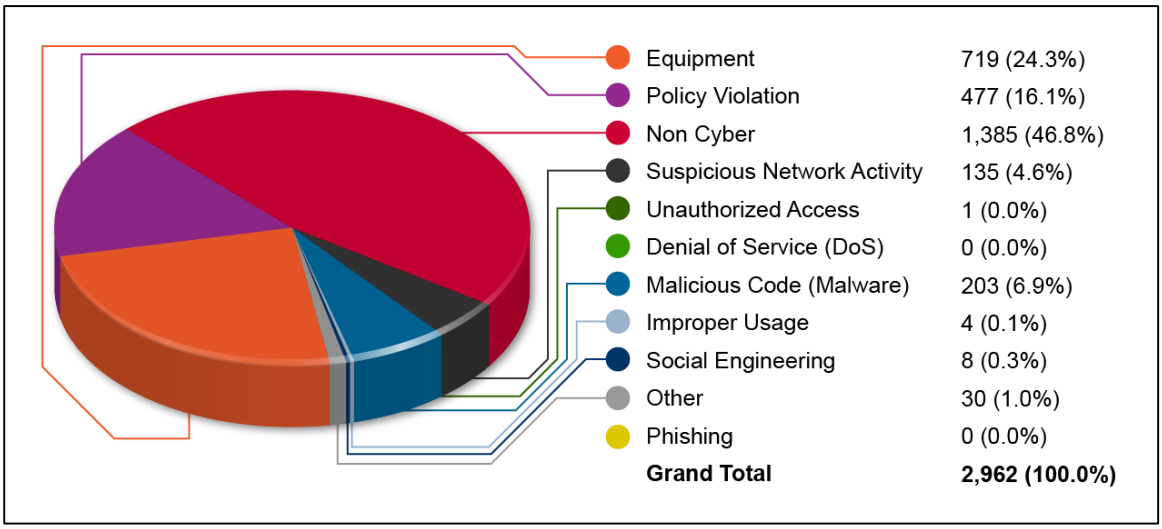
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 28. Security Incidents Reported - Department of State



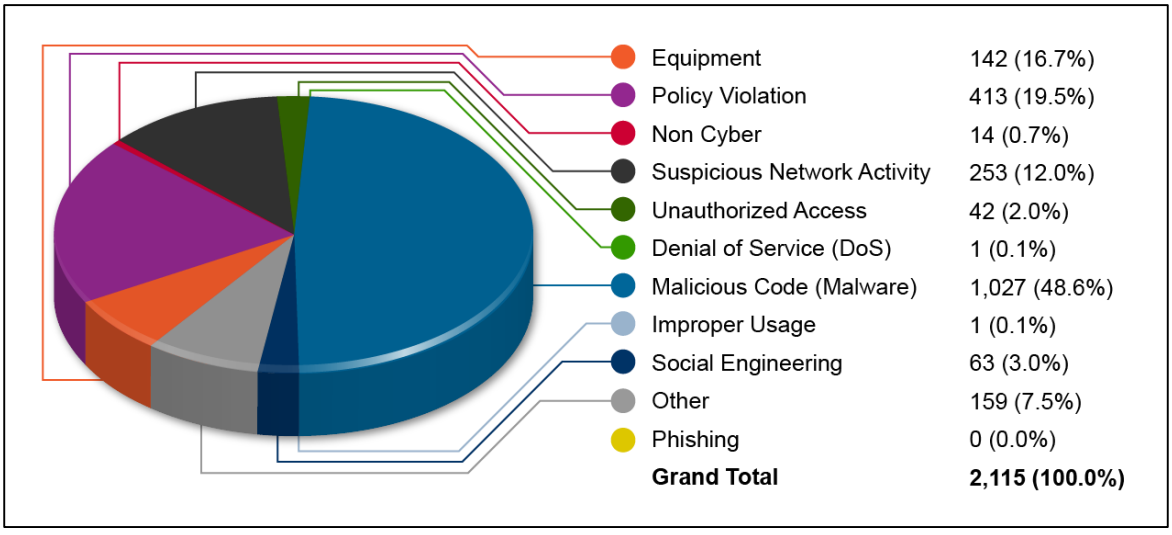
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 29. Security Incidents Reported - Department of the Treasury



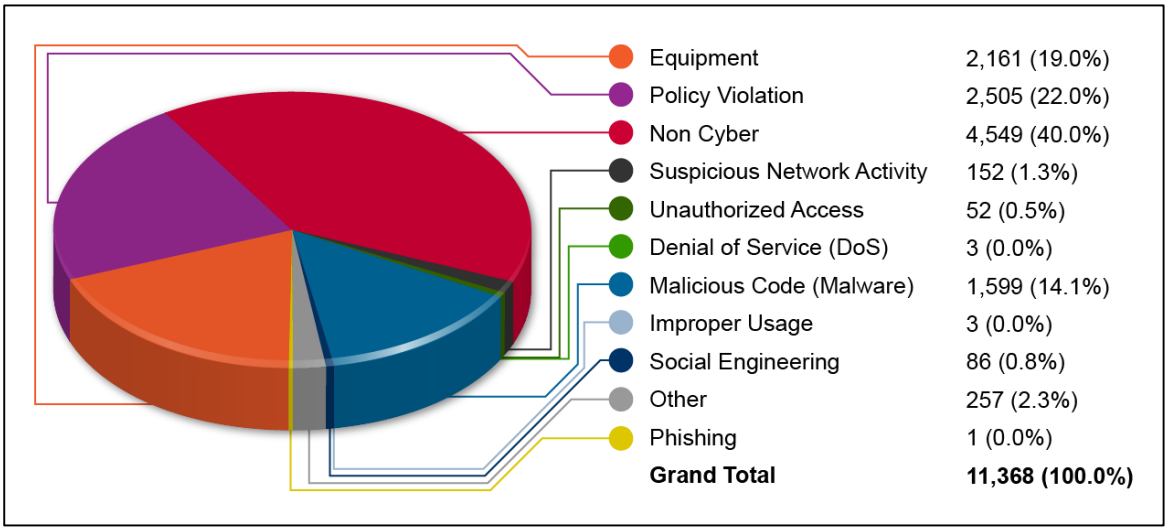
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 30. Security Incidents Reported - Department of Transportation



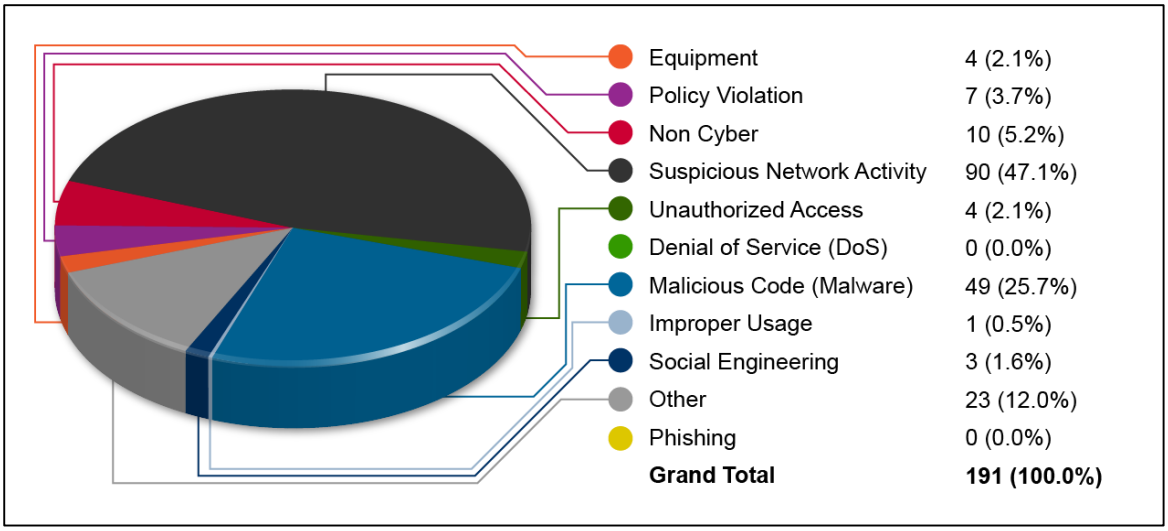
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 31. Security Incidents Reported - Department of Veterans Affairs



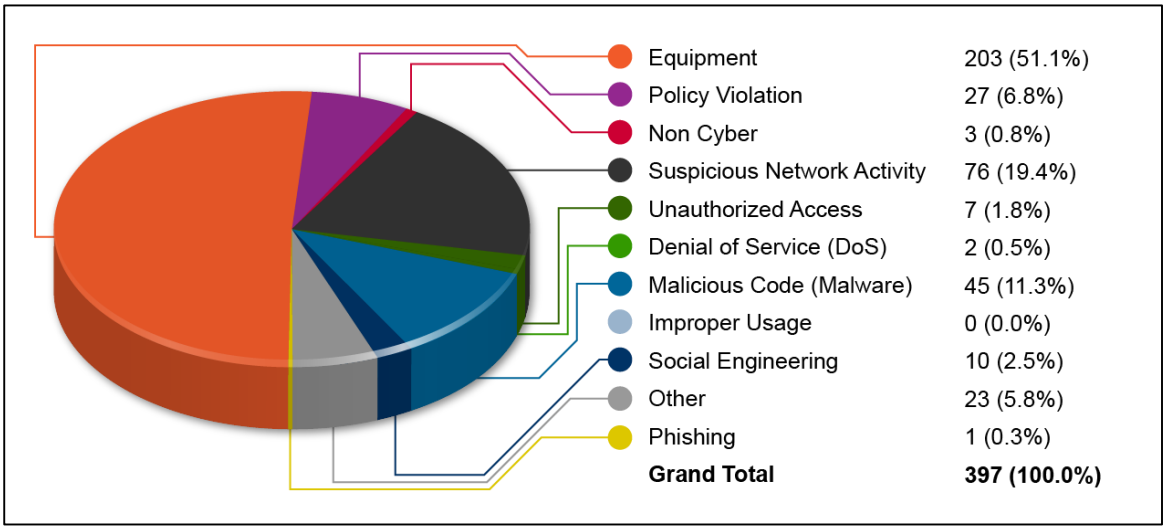
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 32. Security Incidents Reported - Environmental Protection Agency



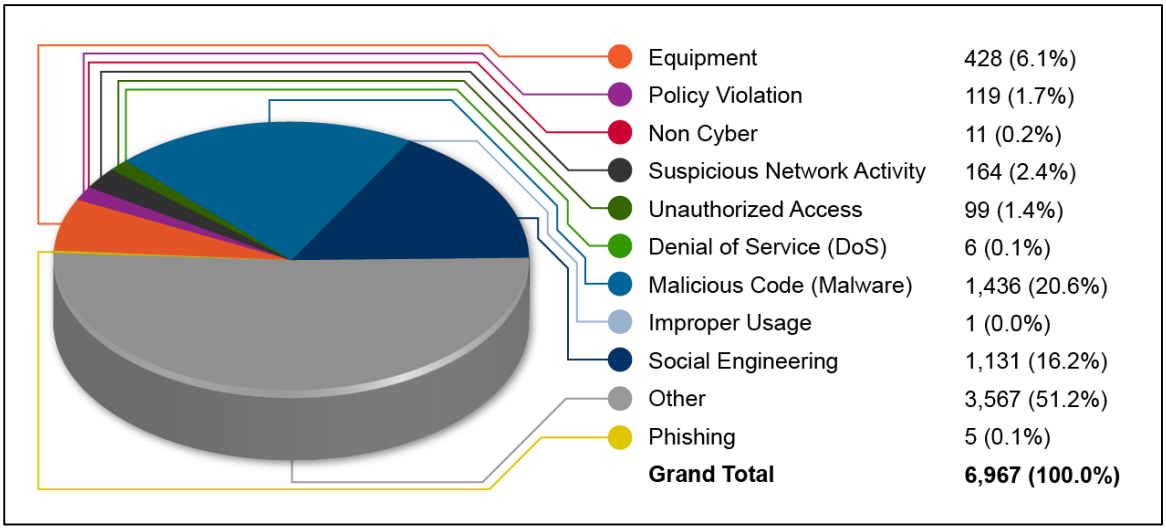
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 33. Security Incidents Reported - General Services Administration



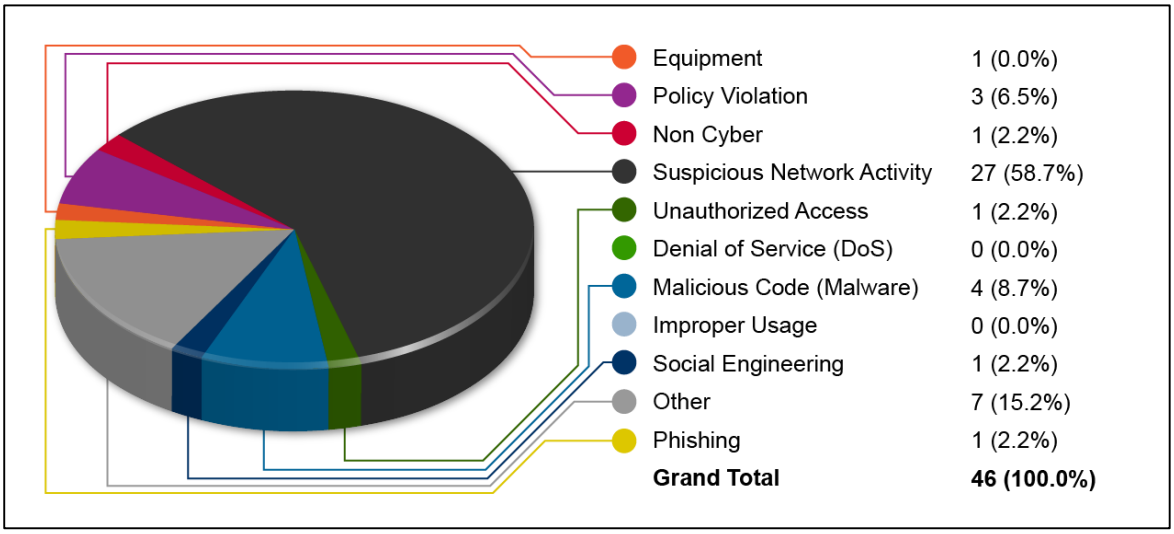
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 34. Security Incidents Reported - National Aeronautics and Space Administration



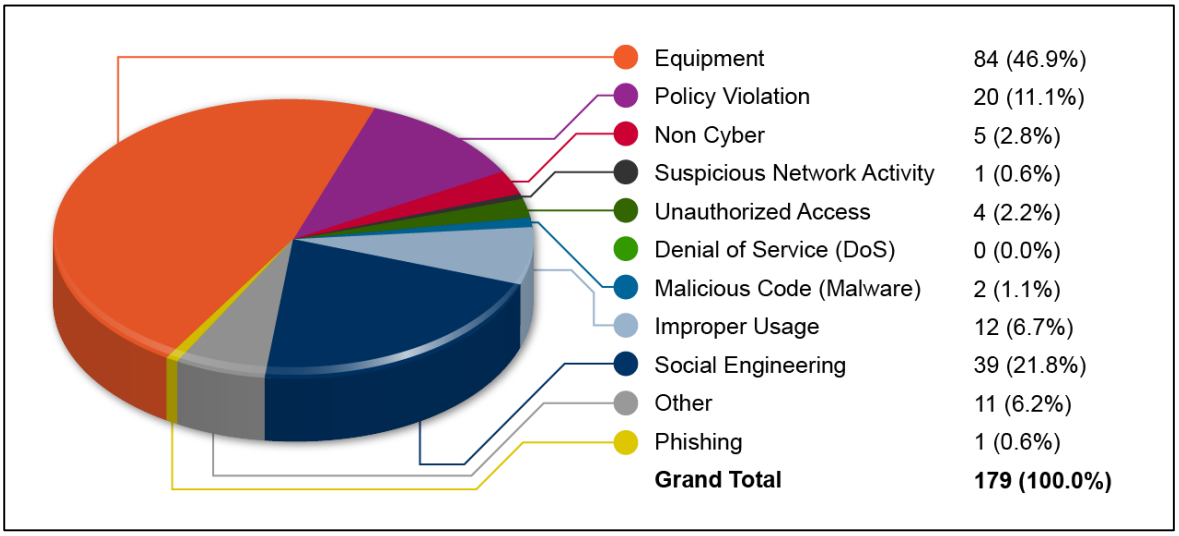
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 35. Security Incidents Reported - National Science Foundation



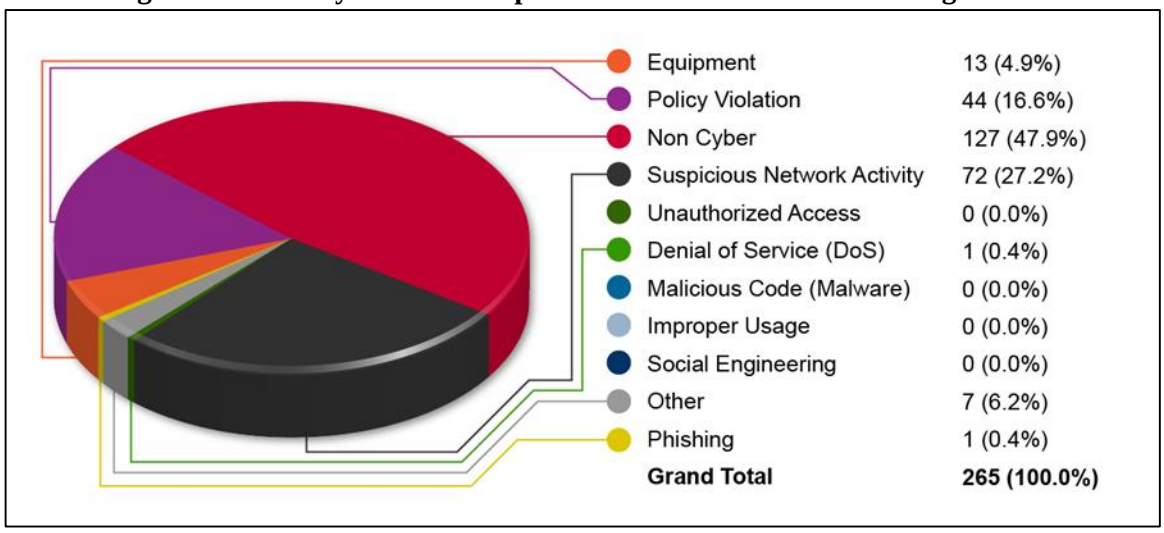
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 36. Security Incidents Reported - Nuclear Regulatory Commission



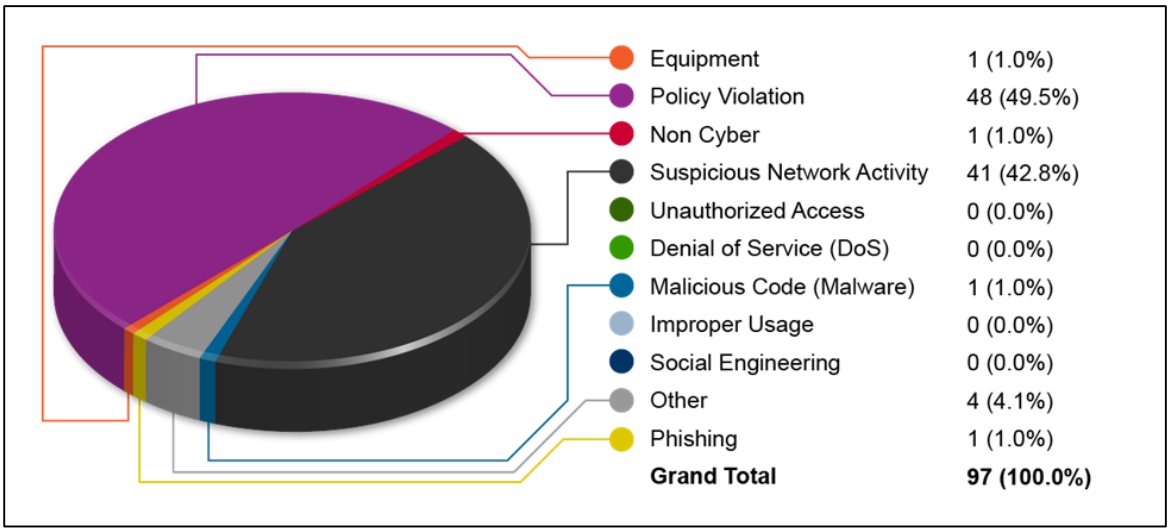
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 37. Security Incidents Reported - Office of Personnel Management



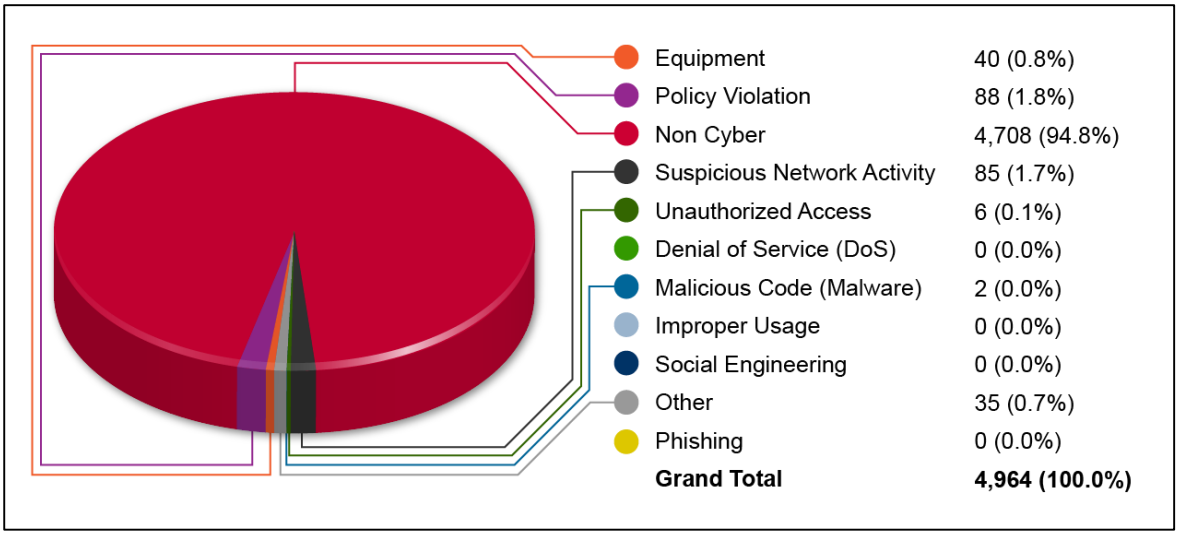
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 38. Security Incidents Reported - Small Business Administration



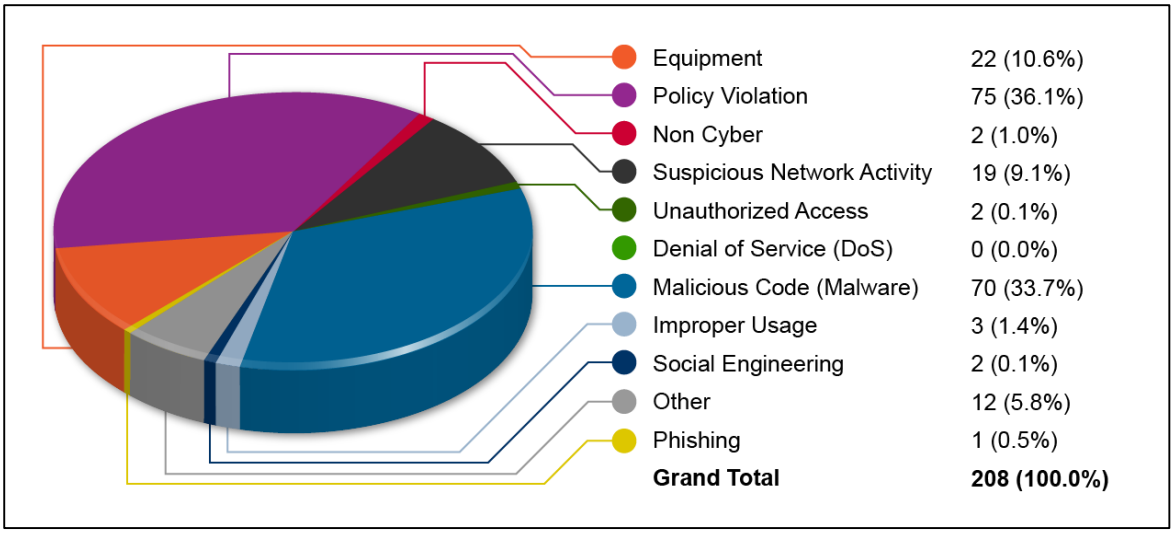
Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 39. Security Incidents Reported - Social Security Administration



Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

Figure 40. Security Incidents Reported - US Agency for International Development



Source: Data reported to US-CERT Incident Reporting System from October 1, 2012 to September 30, 2013.

APPENDIX 3: IT SECURITY SPENDING REPORTED BY CFO ACT AGENCIES

Table 11 shows information security related spending reported by agencies for each of the following key areas: Prevent Malicious Cyber Activity; Detect, Analyze, and Mitigate Intrusions; and Shape the Cybersecurity Environment. Please see Section III for detailed information on these categories.

Table 11. Agency Information Security Spending by Major Category, FY 2013 Actual (Dollars in Millions)

Agency	Prevent Malicious Cyber Activity	Detect, Analyze, and Mitigate Intrusions	Shape the Cybersecurity Environment	Total
Dept. of Agriculture	$39	$23	$1	$63
Dept. of Commerce	$47	$74	$42	$163
Dept. of Education	$11	$11	$0	$22
Dept. of Energy	$112	$69	$37	$218
Dept. of Justice	$105	$335	$6	$446
Dept. of Labor	$5	$9	$9	$23
Dept. of State	$51	$30	$5	$86
Dept. of Transportation	$44	$48	$5	$96
Dept. of Veterans Affairs	$11	$102	$7	$121
Dept. of the Interior	$13	$24	$1	$38
Dept. of the Treasury	$146	$109	$13	$268
Dept. of Defense	$2,471	$1,055	$3,580	$7,106
Dept. of Health & Human Services	$44	$111	$26	$181
Dept. of Homeland Security	$369	$590	$150	$1,109
Dept. of Housing & Urban Development	$4	$7	$0	$12
Environmental Protection Agency	$1	$19	$0	$20
General Services Administration	$28	$10	$8	$46
International Assistance Programs	$8	$7	$7	$22
National Science Foundation	$3	$6	$141	$150
NASA	$27	$40	$19	$86
Nuclear Regulatory Commission	$4	$10	$3	$17
Office of Personnel Management	$2	$5	$0	$7
Small Business Administration	$1	$4	$0	$5
Social Security Administration	$27	$11	$2	$40
Total Information Security Spending	**$3,575**	**$2,707**	**$4,063**	**$10,344**

APPENDIX 4: INSPECTORS GENERAL'S RESPONSE

As described in Section V, each agency Inspector General (IG) was asked to assess his or her department's information security programs in the following areas:

- Continuous monitoring management;
- 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;
- Contractor systems; and,
- Security capital planning.

The IGs were asked to evaluate 99 attributes across these areas and determine whether their agencies established a program for information security in each area. The IGs were then asked to determine whether specific elements were in place for each program. Amongst both the CFO Act agencies and the small and micro agencies the strongest areas were incident response and reporting, security training, plans of actions and milestones, and remote access, while the weakest performances occurred in continuous monitoring management, configuration management, risk management, contractor systems, and contingency planning.

CFO Act Agencies

Table 12 summarizes the results from the IGs of the 24 CFO Act agencies according to cyber security program area. These results indicate that the departments performed best in incident response and reporting, security training, remote access management, and security capital planning. The weakest performances occurred in continuous monitoring management, configuration management, risk management and contingency planning.

Table 12. Results for CFO Act agencies by Cyber Security Area

Cyber Security Program Area	Program in place		Program not in place	
	FY 2013	%	FY 2013	%
Continuous monitoring	17	74	6	26
Configuration management	15	65	8	35
Identity and access management	18	78	5	22
Incident response and reporting	22	96	1	4
Risk management	17	74	6	26
Security training	21	91	2	9
POA&M	20	87	3	13
Remote access management	22	96	1	9
Contingency planning	18	78	5	22
Contractor systems	17	74	6	26
Security capital planning	21	91	2	9

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

Table 13 provides the CFO Act agencies' compliance scores for FY 2013 and FY 2012. The table is organized according to agencies' FY 2013 compliance scores. Ten large agencies had programs in place for all eleven areas, although each identified areas for improvement. The other 13 agencies had at least one area for which it did not have a program. The numbers of areas with deficiencies were used to compute compliance scores. Six agencies scored over 90% compliance, 11 scored between 65% and 90% compliance, and the remaining 6 scored less than 65%. Due to difference between general FISMA metric requirements and DOD program specifications, the DOD OIG requested DOD's score be displayed as "N/A". The average score was 76% for both fiscal years 2013 and 2012, respectively – no significant change.

Table 13. CFO Act agencies' Compliance Scores

Agency	FY 2013 (%)	FY 2012 (%)
Department of Homeland Security	99	99
General Services Administration	98	99
Department of Justice	98	94
Nuclear Regulatory Commission	98	99
Social Security Administration	96	98
National Aeronautics and Space Administration	91	92
Department of Education	89	79
National Science Foundation	88	90

Agency	FY 2013 (%)	FY 2012 (%)
Department of Commerce[6]	87	61
United States Agency for International Development (USAID)	83	66
Office of Personnel Management	83	77
Department of Veterans Affairs	81	81
Department of the Interior	79	92
Environmental Protection Agency	77	77
Department of Labor	76	82
Department of the Treasury	76	76
Department of Energy	75	72
Department of Transportation	61	53
Small Business Administration	55	57
Department of State	51	53
Department of Health and Human Services	43	50
U.S. Department of Argriculture	37	34
Department of Housing and Urban Development	29	66
Department of Defense[7]	N/A	N/A

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

[6] DOC OIG performed a risk assessment and focused its review on a limited number of attributes. The scoring is based on a modified methodology to reflect this.

[7] Due to difference between general FISMA metric requirements and DOD program specifications, the DOD OIG has requested DOD's score be displayed as "N/A"

Small and Micro Agencies

The results for the small and micro agencies were comparable to those of the 24 CFO Act agencies. Table 14 summarizes the results from the IGs of the small and micro agencies according to cyber security program area. These results indicate that the departments performed best in incident response and reporting, security training, plans of action and milestones, and remote access management. The weakest performances occurred in continuous monitoring management, configuration management, identity and access management, risk management, contingency planning, contractor systems, and security capital planning.

Table 14. Results for Small and Micro Agencies by Cyber Security Area

Cyber Security Program Area	Program in place		Program not in place	
	FY 2013	%	FY 2013	%
Continuous monitoring	22	58	16	42
Configuration management	23	61	15	39
Identity and access management	28	74	10	26
Incident response and reporting	31	82	7	18
Risk management	24	63	14	37
Security training	29	76	9	24
POA&M	29	76	9	24
Remote access management	29	76	9	24
Contingency planning	26	68	12	32
Contractor systems	28	74	10	26
Security capital planning	25	66	13	34

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

Table 15 provides the small and micro agencies' compliance scores for FY 2013. The Federal Retirement Thrift Investment Board, Federal Election Commission, and Office of Special Counsel did not provide sufficient information for scoring in FY 2013. Thirteen small and micro agencies had programs in place for all eleven areas, although, like the similarly situated CFO Act agencies, each identified areas for improvement. The other 25 agencies had at least one area for which it did not have a program. The numbers of areas with deficiencies were used to compute compliance scores. Eight agencies scored over 90% compliance, 20 scored between 65 and 90% compliance, and the remaining 10 scored less than 65%. The average score was 70% for fiscal years 2013, which is comparable to the CFO Act agencies.

Table 15. Small and Micro Agencies' Compliance Scores

Agency[8]	FY 2013 (%)
Equal Employment Opportunity Commission	99%
Tennessee Valley Authority	99%
Farm Credit Administration	99%

[8] Federal Retirement Thrift Investment Board, Federal Election Commission, and Office of Special Counsel did not provide the answers with the detail required for scoring for FY 2013.

Agency[8]	FY 2013 (%)
Federal Energy Regulatory Commission	99%
Export-Import Bank of the United States	96%
Federal Housing Finance Agency	95%
Federal Trade Commission	92%
National Endowment for the Arts	92%
Merit Systems Protection Board	88%
Smithsonian Institution	88%
Federal Reserve Board	88%
National Labor Relations Board	87%
National Endowment for the Humanities	87%
Federal Deposit Insurance Corporation	87%
Federal Labor Relations Authority	84%
Millennium Challenge Corporation	84%
Other Defense Civil Programs	84%
National Credit Union Administration	83%
Commodity Futures Trading Commission	81%
Railroad Retirement Board	80%
Securities and Exchange Commission	80%
National Transportation Safety Board	78%
Overseas Private Investment Corporation	74%
Corporation for National and Community Service	72%
Consumer Financial Protection Bureau	72%
Pension Benefit Guaranty Corporation	71%
Court Services and Offender Supervision Agency	71%
Federal Mediation and Conciliation Service	65%
Federal Maritime Commission	54%
International Boundary and Water Commission	53%
International Trade Commission	51%
Broadcasting Board of Governors	50%
Peace Corps	33%
Consumer Product Safety Commission	30%
National Archives and Records Administration	18%
Federal Retirement Thrift Investment Board	N/A
Federal Election Commission	N/A
Office of Special Counsel	N/A

Source: Data provided to DHS via CyberScope from October 1, 2012, to September 30, 2013

THE ELEVEN CYBER SECURITY AREAS

For the 24 CFO Act agencies, the following summarizes the results by the 11 cybersecurity areas.

Information Security Continuous Monitoring

Information security continuous monitoring 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 provides the required real-time view into security control operations, and has become a key focus point for improving Federal information security.

Based on the IGs' reviews, continuous monitoring programs were in place at 17 departments. Twelve IGs reported that their department had all components of a continuous monitoring program in place.

The weaknesses in continuous monitoring management that the remaining IGs most frequently reported were:

- The department lacked documented policies and procedures for continuous monitoring (seven departments);
- The department lacked documented strategies and plans for continuous monitoring (eight departments);
- Ongoing assessments of security controls (system-specific, hybrid, and common) had not been performed based on the approved continuous monitoring plans (ten departments); and,
- Authorizing officials and other key system officials with security status were not provided reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (seven 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 XP, Vista, and 7 to conform to the U. S. Government Configuration Baseline (USGCB). Furthermore, NIST has created a repository of secure baselines for a wide variety of operating systems and devices.

Based on the IGs' reviews, 15 agencies had configuration management programs in place. However, only three IGs reported that his or her department had all of the required attributes of a successful configuration management program. Consequently, this area needs the most improvement of any FISMA metric. The following deficiencies were most common:

- Windows-based components, USGCB secure configuration settings were not fully implemented, and any deviations from USGCB baseline settings are not fully documented (13 departments)
- Patch management process was not fully developed (15 departments);

- Software assessment capabilities were not fully implemented (11 departments); and,

- Configuration-related vulnerabilities, including scan findings, had not been remediated in a timely manner (18 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 their personnel to use PIV cards. This use of PIV cards is a major component of a secure, governmentwide account and identity management system.

Identity and access management was identified as another area in need of improvement. Eighteen IGs reported that their departments had identity and access management programs in place. The most common control weaknesses were:

- The department does not identify all users, including Federal employees, contractors, and others who access organization systems (eight departments);

- The department's multi-factor authentication system was not linked to its PIV program where appropriate (13 departments);

- The department did not ensure that the users are granted access based on needs and separation of duties principles (nine departments); and,

- The department did not ensure that accounts were terminated or deactivated once access was no longer required (15 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. Reports of incidents on unclassified government systems are received and managed by US-CERT. Incidents involving sensitive data, such as personally identifiable information, must also be reported to US-CERT, though there are strict timelines associated with these kinds of incidents.

Incident response and reporting programs were largely compliant. Twenty-two IGs reported that their departments had incident response and reporting programs in place. However, 11 IGs identified at least one missing component. The following deficiencies were most common:

- Reports to US-CERT were not made within established timeframes (seven departments);

- The department does not report to law enforcement within established timeframes (six departments); and,

- The department did not respond to and resolve incidents in a timely manner (five 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.

Seventeen IGs reported that their departments had risk management programs in place. However, only seven of the 17 reported complete programs, while 17 identified at least one missing component. The following deficiencies were most common:

- The department did not address risk from an organizational perspective with the development of a comprehensive governance structure and organization wide risk management strategy as required by NIST Special Publication 800-37, Revision 1 (12 departments);

- The department did not address risk from a mission and business process perspective and was not guided by risk decisions made at the organizational level, as required by NIST Special Publication 800-37, Revision 1 (10 departments);

- The department did not implement the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation (nine departments); and,

- The department did not ensure that information security controls were monitored on an ongoing basis, with assessments of control effectiveness, documentation of system and operation environment changes and security impact analyses of the changes, and reporting on the security state of the system to designated organizational officials (nine departments).

Security Training

FISMA requires all government personnel and contractors to complete annual security awareness training that includes 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.

Twenty-one IGs reported that their departments had compliant programs. Fourteen reported that their departments' programs included all of the required elements. Among the ten 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 (eight 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 (five departments).

POA&M Remediation

When a department identifies 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' information on the weakness's overall risk to the system, and the actions planned to address the risk, associated costs, and expected completion dates.

Twenty IGs reported that their departments had POA&Ms in place. Of these 20, nine also indicated that their departments' programs had all of the required attributes. Of the 15 IGs indicating that their programs needed improvements, these following issues were most common:

- The department did not track, prioritize and remediate weaknesses (eight departments);
- The department did not ensure remediation plans were effective for correcting weaknesses (nine departments);
- The department had not established and adhered to milestone remediation dates (12 departments); and,
- Costs associated with weakness remediation were not identified (six 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-two IGs reported that their departments had remote access management programs in place, and nine of these had all required attributes. The remaining IGs reported that their departments were missing at least one attribute of a remote access management program. The most common remote access weaknesses were:

- The department lacked documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (eight departments);
- The department did not uniquely identify and authenticate all users for all access (seven departments); and
- Multi-factor authentication was not required for remote access (five 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, seven 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 nine reported that their departments' contingency planning programs were fully compliant with standards. The following issues were prevalent among the 15 departments that needed improvements:

- The department had not performed an overall Business Impact Analysis (nine departments);
- Neither regular ongoing testing nor exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans was performed (ten departments); and,
- Alternate processing sites were subject to the same risks as primary sites (five 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 government information. Consequently, these systems require oversight by the departments that own or use them to ensure that they meet all applicable requirements.

Seventeen IGs reported that their departments had programs in place to manage contractor systems, but only eight reported that their departments' programs included all required attributes. Sixteen 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 (11 departments); and,
- The department had contractor owned or operated systems, some residing in public cloud, that were not compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (nine departments).

Security Capital Planning

Planning for and funding system security must be managed at a department's highest level. Security requirements must be identified, resources estimated, and business cases established to ensure that appropriate levels of security are funded.

Twenty-one IGs reported that their departments had security capital planning programs in place, and 15 of these included all required attributes. Nine IGs reported that their departments had programs in place, but they needed improvements. The most commonly reported weaknesses were:

- The department lacked documented policies and procedures to address information security in the capital planning and investment control (CPIC) process (four departments); and,
- The department's program does not ensure that information security resources are available for expenditures planned (seven departments).

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 DOJ to handle manual and automated inputs of agency data for FISMA compliance reporting.

Non-CFO Act Agency	Acronym
Armed Forces Retirement Home	AFRH
Broadcasting Board of Governors	BBG
Chemical Safety Board †	CSB
Commission on Civil Rights	CCR
Commission of Fine Arts †	CFA
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 †	DC
Equal Employment Opportunity Commission	EEOC
Export-Import Bank of the United States	EXIM
Farm Credit Administration †	FCA
Federal Deposit Insurance Corporation *	FDIC
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
International Boundary and Water Commission	IBWC
International Trade Commission	USITC
Marine Mammal Commission †	MMC
Merit Systems Protection Board	MSPB
Millennium Challenge Corporation	MCC
Morris K. Udall Foundation	MKUF
National Archives and Records Administration	NARA
National Capital Planning Commission †	NCPC
National Council on Disability †	NCD

Non-CFO Act Agency	Acronym
National Credit Union Administration	NCUA
National Endowment for the Arts	NEA
National Endowment for the Humanities	NEH
National Gallery of Art	NGA
National Labor Relations Board *	NLRB
National Transportation Safety Board	NTSB
Nuclear Waste Technical Review Board †	NWTRB
Occupational Safety and Health Review Commission	OSHRC
Office of Government Ethics †	OGE
Office of Navajo and Hopi Indian Relocation †	ONHIR
Office of Special Counsel	OSC
Other Defense Civil Programs	ODCP
Overseas Private Investment Corporation	OPIC
Peace Corps	PC
Pension Benefit Guaranty Corporation	PBGC
Postal Regulatory Commission † *	PRC
Railroad Retirement Board	RRB
Recovery Act Accountability and Transparency Board	RAATB
Securities and Exchange Commission *	SEC
Smithsonian Institution	SI
Tennessee Valley Authority	TVA
United States Interagency Council on Homelessness	USICH

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

END NOTES

i. Title III of the E-Government Act of 2002 (P.L. 107-347) is available at: *www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf*

ii. OMB Memorandum M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," (July 6, 2010), available at: *www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf*

iii. OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," (November 18, 2013), available at: *www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf*

iv. Information regarding DHS Trusted Internet Connections is available at: *www.dhs.gov/trusted-internet-connections*

v. Information regarding DHS Privacy Impact Assessment for Einstein 2 is available at: *www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf*

vi. The Federal CIO Council and DHS National Protection and Program Directorate, Office of Cybersecurity and Communications (Federal Network Resilience), "Mobile Security Reference Architecture" is available at: *www.cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf*

vii. The Cross Agency Priority Goal: Cybersecurity, FY 2013 Q4 Update is available at: *www.goals.performance.gov/sites/default/files/images/Cybersecurity_CAP_Goal_FY13Q4_FINAL.pdf*

viii. Information concerning GSA Multiple Award IT Schedule 70 is available at: *www.gsa.gov/portal/content/104506?utm_source=FAS&utm_medium=print-radio&utm_term=schedule70&utm_campaign=shortcuts*

ix. Homeland Security Presidential Directive12, "Policy for a Common Identification Standard for Federal Employees and Contractors," (August 27, 2004), available at: *www.dhs.gov/homeland-security-presidential-directive-12#1*

x. The 2009 Cyberspace Policy Review is available at: *www.WhiteHouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*

xi. OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors," (February 3, 2011), available at: *www.WhiteHouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf*

xii. See NIST Federal Information Processing Standard 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors" at: *http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf*

xiii. Executive Order 13587, " Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," (October 7, 2011) is available at: *www.WhiteHouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-*

classified-networks-

xiv. Presidential Memorandum, "Building a 21st Century Digital Government," (May 23, 2013), available at: *www.WhiteHouse.gov/the-press-office/2012/05/23/presidential-memorandum-building-21st-century-digital-government*

xv. See NIST Special Publication 800-124 Revision 1, "Guidelines for Managing and Securing Mobile Devices in the Enterprise," at: *http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf*

xvi. See Draft NIST Special Publication 800-164, "Guidelines on Hardware-Rooted Security in Mobile Devices," at: *http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf*

xvii. See NIST Special Publication 800-73, "Interfaces for Personal Identity Verification," at: *http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf*

xviii. The 25 Point Implementation Plan to Reform Federal Information Technology Management is available at: *www.WhiteHouse.gov/sites/default/files/omb/assets/egov_docs/25-point-implementation-plan-to-reform-federal-it.pdf*

xx. Federal CIO Memorandum, "Security Authorization of Information Systems in Cloud Computing Environments," (December 8, 2011), available at: *https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf*

xxi. See NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," at: *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

xxii. The National Strategy for Trusted Identities in Cyberspace is available at: *www.WhiteHouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*

xxiii. NIST FIPS 140-2, "Security Requirements for Cryptographic Modules," is available at: *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*

xxiv. OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," (June 23, 2006), available at: *www.WhiteHouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf*

xxv. OMB Memorandum M-08-23, " Securing the Federal Government's Domain Name System Infrastructure," (August 22, 2008), available at: *www.WhiteHouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf*

xxvi. Information regarding the US-CERT Incident Reporting System is available at: *www.us-cert.gov/forms/report*