Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

March 2013

Table of Contents

List of Figures

List of Tables

I. Introduction: Current State of Federal Information Security

The Federal Government provides thousands of essential services to the public, ranging from disaster assistance, to social security, to national defense. To efficiently provide these services to the public, the Federal Government relies on safe, secure, and resilient Information Technology (IT) infrastructure. Threats to Federal information – whether from insider threat, criminal elements, or nation states – continue to grow in number and sophistication, creating risks to the reliable functioning of our government. The Federal Government has a duty to protect against these threats and secure Federal information and information systems. This responsibility is codified in the Federal Information Security Management Act (FISMA)[1], which requires agencies to provide information security protections commensurate with risks and their potential harms to federal information. It also gives the Office of Management and Budget (OMB) the responsibility of overseeing agency information security policies and practices, and the National Institute of Standards and Technology (NIST) the responsibility of prescribing standards and guidelines pertaining to Federal information systems. In 2010, the Office of Management and Budget (OMB) issued Memorandum 10-28[2] providing the Department of Homeland Security (DHS) an expanded role with respect to the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA.

The Administration's cybersecurity priorities identified in 2011 – Trusted Internet Connections, Continuous Monitoring and Strong Authentication leveraging Homeland Security Presidential Directive 12 (HSPD-12) – were designated as Cross Agency Priority (CAP) Goals in 2012 consistent with the Government Performance and Results Modernization Act (GPRA Modernization Act).[3] In selecting the goals, emphasis was placed on Presidential priorities and where increased cross-agency coordination and regular review would be expected to speed progress. For these reasons, the Administration identified cybersecurity as a CAP goal.

The three priority areas identified for improvement within Federal cybersecurity (Trusted Internet Connections, Continuous Monitoring and HSPD-12) are based on long-standing Federal initiatives. The Federal Government established these priorities to examine what data and information is entering and exiting agency networks (Trusted Internet Connections, or TIC); what components are on agency information networks and when their security status changes (continuous monitoring); and who is on agency systems (strong authentication using HSPD-12 Personal Identity Verification credentials). Progress on these priorities is included in Sections II and IV of this report. This Fiscal Year (FY) 2012 FISMA Report to Congress, as required in 44 USC 3543, also provides the annual status of government-wide and agency-specific information security initiatives with respect to compliance with FISMA requirements. Accomplishments, in FY 2012 included:

- In May 2012, the President issued a directive entitled "Building a 21st Century Digital Government". This launched a comprehensive Digital Government Strategy aimed at delivering better digital services to the American people and requires the integration of

---

[1] Title III of the E-Government Act of 2002 (Pub. L. No. 107-347).

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

[3] To enhance progress in areas needing more cross-agency collaboration, the GPRA Modernization Act requires OMB to establish a limited number of CAP Goals for both crosscutting policy and government-wide management areas.

effective security and privacy measures into the design and adoption of all new technologies introduced to the Federal environment.

- Established the interagency Joint Continuous Monitoring Working Group to support Federal agencies' efforts to build a government-wide continuous monitoring capability for Federal information systems.
- Conducted multiple agency CyberStat reviews to help Federal agencies improve cybersecurity performance by identifying the cybersecurity capability areas where they may have faced organizational implementation roadblocks (e.g., technology challenges, organizational culture, internal processes, or human capital/financial resource challenges) and collaborating to break down those barriers.
- Incorporated Cybersecurity considerations into PortfolioStat reviews during summer of 2012. Under PortfolioStat, agencies and OMB engage collaboratively to analyze and improve agency IT portfolios, addressing agency-wide management opportunities and challenges.
- Collaborated with Federal agencies to release the FY 2013 FISMA metrics, focusing on accountability, visibility, and automation to make meaningful and measurable improvements in system security.
- Stood up the National Cybersecurity and Communications Integration Center at the Department of Homeland Security to coordinate cyber incident response.
- Updated the implementation strategy for the Einstein 3 intrusion prevention system to enable significant capabilities to be deployed during FY 2013, four years earlier than planned.
- Held a cyber-focused National Level Exercise (NLE) and integrated lessons learned into Federal information security management programs. The NLE 2012 is part of a series of congressionally mandated preparedness exercises designed to educate and prepare participants for potential catastrophic events. The NLE 2012 process examined the nation's ability to coordinate and implement prevention, preparedness, response and recovery plans and capabilities pertaining to a significant cyber event or a series of events.
- Released the "National Strategy for Information Sharing and Safeguarding"[4] as part of the Wikileaks incident response and in an effort to establish government-wide policy. The policy strikes the proper balance between sharing information with those who need it to keep our country safe, while safeguarding information from those who would do our country harm. The Strategy recognizes that information security and information sharing are mutually reinforcing activities, through three guiding principles:
    - Information is a national asset;
    - Information sharing and safeguarding requires shared risk management; and
    - Information informs decision making.
- Released the "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs". This policy directs and guides agencies to develop and promote effective insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat to national security.

[4] Located at: http://www.whitehouse.gov/the-press-office/2012/12/19/national-strategy-information-sharing-and-safeguarding

II. Key Ongoing Information Security Initiatives

The Federal information security defensive posture is a constantly moving target, shifting due to a relentless, dynamic-threat environment, emerging technologies, and new vulnerabilities. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation. Based on information reported by US-CERT, in Section III, malicious code continues to be one of the most widely reported incident types across agencies and measures are being taken to identify and mitigate weaknesses in the Federal infrastructure that can be exploited by malware. As the Federal workforce gravitates to increased teleworking and remote access, initiatives are underway to address unauthorized access and equipment incidents. A workforce instilled with cybersecurity competencies can help defend against social engineering, phishing, and insider threat attacks. Improper usage, policy violations, and non-cyber incidents, which can lead to the unauthorized disclosure of Personally Identifiable Information (PII), is also a key focus area.

Given the range of potential threats, Federal agencies need to focus their information security activity on the most cost-effective and efficient controls relevant for their organizations and related mission needs. This section discusses the collective efforts of Federal agencies, in conjunction with Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and Executive Office of the President components, such as Office of Management and Budget (OMB) and National Security Staff (NSS), to improve the Federal Government's information security posture. Improving our information security posture will require a vigorous and extensive build-out of technical and policy protection mechanisms for government systems, a growing and robust partnership with the private sector, and a focus on interagency cooperation. We must focus on protecting our assets and supporting safe and secure adoption of emerging technologies, while building a 21st century workforce, and improving cost effectiveness across the Federal enterprise.

The initiatives described in the remainder of this section represent key efforts under way in FY 2012; we expect them to carry forward into FY 2013.

A. Protecting Our Assets

The Federal Government continues to be vigilant in protecting our nation's information assets. Trusted Internet Connections (TIC), Continuous Monitoring (CM) and strong authentication measures using HSPD-12 Personal Identity Verification (PIV) credentials help ensure that federal information remains secure. CyberStat reviews, in-depth sessions with NSS, OMB, DHS and the selected agency, discuss that agency's cybersecurity posture and discuss opportunities for collaboration. Risk and Vulnerability Assessments (RVA) of agencies by independent parties provide assessments that lead to proactive corrections. Unauthorized disclosure of and access to sensitive information is one of our highest concerns and is being addressed through multiple programs.

Trusted Internet Connections

The purpose of the TIC initiative is to improve the federal government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections. This is accomplished by establishing TIC Access Provider (TICAP). Each TICAP has baseline security capabilities including firewalls, malware policies, and network/security operation centers. The National Cybersecurity Protection System (NCPS) EINSTEIN 2 capability is also being deployed at each TICAP. EINSTEIN 2 is an Intrusion Detection System (IDS) capability that alerts when a specific cyber threat is detected, which allows US-CERT to analyze malicious activity occurring across the Federal IT infrastructure resulting in improved computer network security situational awareness.

Through FY 2010 and FY 2011, DHS worked with an inter-agency group of subject matter experts to update the TIC baseline security capabilities in the TIC architecture, based on evolving and increasingly sophisticated threats. TICAPs and Managed Trusted Internet Protocol Services (MTIPS) providers are now implementing TIC v2.0, in coordination with other network changes needed to support Internet Protocol version 6 (IPv6). In FY 2013, DHS will work with agencies to develop the TIC v2.1 reference architecture focusing on mobile computing and cloud services.

Einstein 3

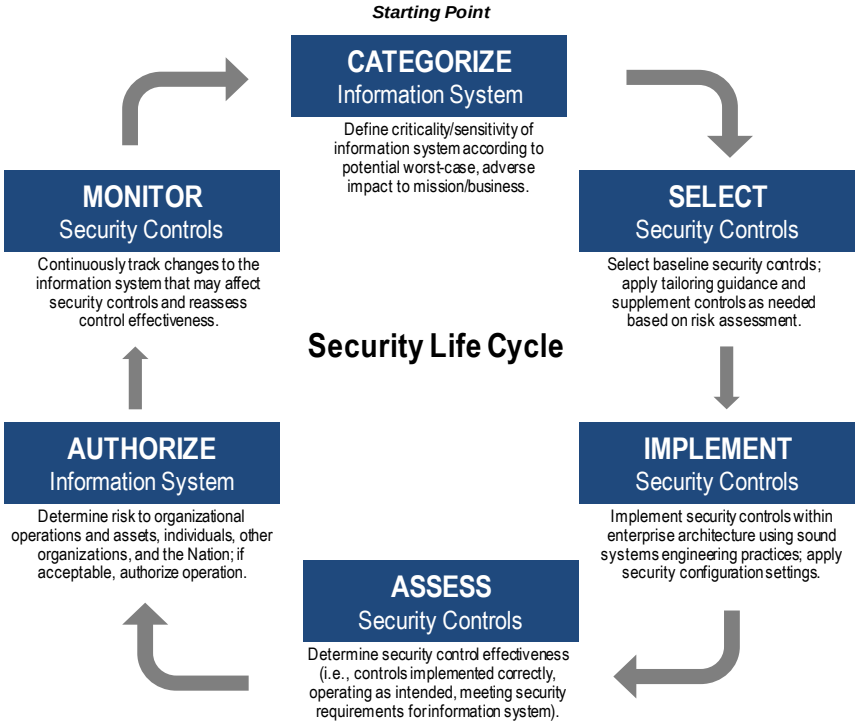
In FY 2013, DHS expects to begin deployment of the NCPS EINSTEIN 3 capability as a managed security service. Einstein 3 provides intrusion prevention capabilities to disable attempted intrusions before harm is done and conduct threat-based decision making on network traffic entering or leaving Federal Executive Branch civilian networks. EINSTEIN 3 augments the capabilities under EINSTEIN 2 and will provide US-CERT and agency CERT teams with an increased set of defensive capabilities to detect, collect, act upon and report on cybersecurity events in near real-time. Through this effort, DHS aims to further improve the agencies' security posture and incident response capabilities.

Continuous Monitoring

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Continuous monitoring is one of the major components of the six-step Risk Management Framework (RMF) as published in the NIST SP 800-37, Revision 1, *"*Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*"*[5]. Figure 1 below illustrates the RMF processes that provide the foundation for an information system's security life cycle.

[5] Chapter Three of NIST Special Publication 800-37 Revision 1 describes the six steps of the Risk Management Framework. More details can be found here: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Figure 1. Risk Management Framework Overview



Continuous monitoring is an integral part of an enterprise-wide risk management process that allows agencies to establish the context of their risk management programs, and subsequently assess risk, respond to risk, and monitor risk on an ongoing basis.[6] Continuous monitoring programs are most effective when combined with other agency initiatives to strengthen the underlying information technology infrastructure by integrating security requirements into organizational processes (e.g., enterprise architecture, acquisition/procurement, systems engineering, and the system development life cycle).

OMB, DHS and NIST are working together to define a standards-based approach for continuous monitoring capabilities, developing viable and cost-effective approaches to measure capabilities derived from continuous monitoring data which will address concerns about exposure of operational data and standardize the consistency of reporting. This approach will provide a platform for robust and unambiguous technical data to be better harnessed and will provide essential, near real-time security status-related information.

A key component to this work is the NIST Security Content Automation Protocol (SCAP) and related programs, which are developed through close collaboration between government and industry partners, to provide the standardized technical mechanisms to share information between systems, supporting automated vulnerability checking, technical control compliance activities, and security measurement. To encourage increased adoption for commercial products and to provide increased interoperability, NIST will work with industry and international standards organizations

[6] NIST Special Publication 800-39, "Managing Information Security Risk", provides guidance on the risk management process and the role of continuous monitoring.

to promote adoption of open standards to allow for this technical data to be extended, managed, and shared federally, commercially, and internationally.

In 2012, DHS also continued work on its Continuous Diagnotistics and Mitigation Program, to support agency's implementation of Continuous Monitoring. The DHS continuous diagnostics program is one of the key components in a comprehensive continuous monitoring program. Therefore, it will be based upon NIST standards and guidelines including SP 800-30[7], SP 800-37[8], SP 800-39[9], SP 800-53[10], and SP 800-53A[11]. This program will monitor, in collaboration with other agencies, a specific subset of security controls from organizational security plans to obtain critical information on the security status of Federal information systems (i.e., diagnose specific problems relating to security control effectiveness or the loss or degradation of a security capability).

Under NIST guidelines, agencies have a responsibility to ensure that all security controls (including those controls designated by DHS), are monitored on an ongoing basis. The DHS continuous diagnostics program will help define the frequency, rigor, and extent of such monitoring activities for those security controls associated with the program. Continuous monitoring of all security controls is necessary to ensure that agencies provide a breadth and depth of security capabilities to support a defense-in-depth strategy, and that the controls that are part of that strategy remain effective over time.

In late 2012, DHS released a Request for Proposal to support its Continuous Diagnostics and Mitigation (CDM) program of providing continuous monitoring sensors, diagnosis, mitigation tools, and Continuous Monitoring as a Service (CMaaS). The service will include a reporting dashboard that provides visualizations of agency risks and promotes a quick resolution to issues discovered.

The DHS continuous diagnostics procurement is intended to be widely applicable to support Federal information systems, and Federal information hosted by others (e.g., cloud service providers). DHS plans to pilot initial continuous diagnostics metrics during FY 2013 to help determine benefit and impact to help each agency improve its continuous monitoring capability.

The DHS continuous diagnostics program aims to increase visibility into the security status of Federal information systems and environments of operation. The program can also enhance DHS's ability to assess agency security control effectiveness, and assist organizational personnel in identifying and responding to intrusions in their operational environments. In addition to the above, the continuous diagnostics program aims to support information system owners, common control providers, and authorizing officials with some of the necessary information to:

---

[7] NIST Special Publication 800-30, "Guide for Conducting Risk Assessments", at: http://csrc.nist.gov/publications/PubsSPs.html

[8] NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", at: http://csrc.nist.gov/publications/PubsSPs.html

[9] NIST Special Publication 800-39, "Guide for Managing Information Security Risk", at: http://csrc.nist.gov/publications/PubsSPs.html

[10] NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations", at: http://csrc.nist.gov/publications/PubsSPs.html

[11] NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations", at: http://csrc.nist.gov/publications/PubsSPs.html

- Manage the highest priority and most serious risks addressed by the subset of security controls monitored by the DHS continuous diagnostics program based on risk assessment information and the risk tolerance established by individual departments and agencies;
- Help agencies share or transfer risk, if appropriate;
- Improve the effectiveness and efficiency of continuous monitoring programs; and
- Improve the maturity of continuous monitoring programs across the Federal government.

These capabilities will be rolled up into an extensible dashboard[12] for agency-level and Federal government-wide views. A standard set of "dashboards" will help agencies use the data on a daily basis to find and fix their highest priority defects. This dashboard will also automate Cyberscope data feeds, and allow for more frequent transmission.

Sensor data feeds will be implemented in accordance with existing, installed agency continuous monitoring capabilities. Currently, many of these existing continuous monitoring systems report to Cyberscope through a manual process that will need to be automated. For agencies without an existing continuous monitoring capability, the DHS continuous diagnostics program will assist in addressing that gap.

Strong Authentication: HSPD-12

The 2009 Cyberspace Policy Review, issued at the direction of the President, highlighted the importance of identity management in protecting the nation's infrastructure. HSPD-12, issued in August 2004, is a strategic initiative intended to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. HSPD-12 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. Specific benefits of the standardized credentials required by HSPD-12 include multi-factor authentication and digital signature and encryption capabilities.

With the majority of federal employees and contractors having received PIV smartcard credentials, in FY 2012, the Federal Government continued to focus on leveraging the electronic capabilities of the PIV cards. This effort builds on OMB Memorandum M-11-11, "Continued Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,[13]" issued in February 2011. This memorandum outlined a plan of action to expedite the Executive Branch's full use of the credentials and 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. To be effective in achieving the goals of HSPD-12, and realizing the full benefits of PIV credentials, the memorandum outlined specific requirements to be addressed in the agency policy.

---

[12] The dashboards associated with the continuous diagnostics program are designed to be extensible in order to include other risk-related information (reflecting security controls implemented to address management and operational vulnerabilities) necessary to develop a more comprehensive view of department and agency risk postures.

[13] OMB 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, is located at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

To support this effort, the Federal Chief Information Officer (CIO) Council and OMB developed a segment architecture and implementation guidance[14] for Identity, Credential, and Access Management (ICAM). This common government-wide architecture supports the enablement of ICAM systems, policies, and processes to facilitate business amongst federal agencies and between the federal government and its business partners and constituents. The architecture provides Federal agencies with a consistent approach for planning and executing ICAM programs as well as a comprehensive guide to achieving the target state of their programs. The implementation of ICAM is leading to several benefits including: increased security; improved compliance with laws, regulations and standards; improved interoperability; enhanced customer services; elimination of redundancy; and increased protection of personally identifiable information. ICAM improves information security posture across the Federal Government through standardized and interoperable identity and access controls. The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. The document includes addendums that speak to the best practices of new approaches and technologies prior to their adoption within the agencies. Agencies are required, by OMB M-11-11, to align with the ICAM roadmap in their implementation of HSPD-12.

Additionally, the Department of Commerce National Institute of Standards and Technology (NIST) is in the process of finalizing revision 2 of the HSPD-12 standard, FIPS 201,[15] to address the integration of PIV credentials with mobile devices and advances in technology. In support of this effort, NIST is also working on a new Special Publication 800-157, titled "Guidelines for Personal Identity Verification (PIV) Derived Credentials."

CyberStat

DHS, along with the OMB and the White House National Security Staff, continued to conduct CyberStat reviews of selected agencies in FY 2012. CyberStat reviews are face-to-face, evidence-based meetings to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing focused strategies for improving information security posture. During FY 2012, CyberStat reviews were conducted with the following seven agencies: Department of Justice; Office of Personnel Management; United States Agency for International Development; Department of Agriculture; Department of Transportation; Department of Labor, and the National Aeronautics and Space Administration.

DHS performed an overall analysis of the agencies data selected for an FY 2012 CyberStat Review and is continuing to work with the selected agencies to identify and correct weaknesses in their cybersecurity programs. The reviews provided the opportunity for agencies to identify the cybersecurity capability areas where they were facing implementation maturity challenges. The top challenges raised by agencies include: organizational 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. In addition, CyberStat Reviews highlighted

[14] A copy of the "Federal Identity, Credential and Access Management Roadmap and Implementation Guidance Version 2.0" is located at: http://www.idmanagement.gov.

[15] A copy of the draft "FIPS 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors" is located at: http://csrc.nist.gov/publications/PubsFIPS.html.

areas where agencies are meeting and exceeding requirements that enabled DHS to put forward best practices to other agencies.

DHS worked in collaboration with agency Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) and carefully examined agency-specific cybersecurity program data. The intended outcome is to present a time sensitive, prioritized action plan for the agency, informed by current operational challenges and events, to improve overall agency performance. All actions from the CyberStat Reviews are followed to closure. Since the CyberStat Reviews began, agencies have improved their progress by resolving various issues, identifying the need for assistance from General Services Administration (GSA) surrounding asset purchases, and interacting with other agencies to leverage best practices. Additionally, OMB has assisted in coordinating meetings with agency top leadership to address funding issues.

The CyberStat Reviews present the opportunity to stress to agencies the Cross Agency Priority goals for cybersecurity and the metrics emphasized by the Administration. These include the metrics constituting continuous monitoring, TIC compliance and traffic consolidation, and HSPD-12 implementation. The metrics data for the Cross Agency Priority goals used in the CyberStat Reviews was shared with the President's Management Council (PMC) and the Secretaries of the Departments. The PMC provides the opportunity to engage the Deputy Secretaries of the Chief Financial Officer (CFO) Act agencies to have them assist in driving implementation progress towards key strategic enterprise cybersecurity capabilities. For the civilian agencies that did not undergo a CyberStat review in FY 2012, DHS met with the agency CIO and CISO on their agency's security posture. These sessions were designed to assist the assessment of the agency's FISMA compliance and challenges, identifying security best practices and raising awareness of FISMA reporting requirements while establishing meaningful dialogue with the agency's senior leadership. The analysis from these meetings in FY 2011 enabled DHS to track trends in the agencies' strategies to ensure a consistent focus of security vulnerabilities and threats, and these were addressed in follow-up meeting in FY 2012. As this engagement continues in FY 2013, identification of these trends will aid DHS continued actions to improve the overall security posture of the Federal Government.

Conducting Risk and Vulnerability Assessments

Risk and Vulnerability assessments entail working with organizations to analyze and independently test their systems for vulnerabilities using tools and tactics comparable to those of a malicious third party. DHS is targeting the civilian agencies with a suite of in-depth Risk and Vulnerability Assessment (RVA) services that will provide a detailed evaluation of their technical capabilities (tools and technologies) and operational readiness (people, processes, and security program maturity). Assessed agencies will receive an objective risk analysis report that quantifies their specific threats and vulnerabilities and provides a prioritized list of suggested remediation actions to achieve the greatest return on investment for the agency.

By proactively engaging with agencies and providing security services designed to assist them in establishing, communicating, and continuously improving their cybersecurity postures, DHS aims to improve the cybersecurity preparedness of the Federal Government and reduce the risk of malicious compromise of Federal systems and information.

Information Sharing and Safeguarding to Prevent Unauthorized Disclosure

The Administration has continued to provide a priority focus on preventing the unauthorized disclosure of Federal Government information in the face of increasingly sophisticated internal and external threats. Executive Order 13587 (October 2011) established a Senior Executive Information Sharing and Safeguarding Steering Committee that is co-chaired by the National Security Staff and the Office of Management and Budget to coordinate policy regarding the sharing and safeguarding of classified and sensitive information throughout the Federal Government from exploit, compromise, and unauthorized disclosure. The Order also established an Insider Threat Task Force (ITTF) to deter, detect, and mitigate insider threats government-wide.

The Steering Committee coordinates with a number of other focused groups, including:

- The National Security Staff's Information Sharing and Access Inter-agency Policy Committee (ISA-IPC) which serves as a focal point for a broad range of information sharing issues that impact national security.
- The Director of National Intelligence's Program Manager for the Information Sharing Environment (PM-ISE) plans, manages, and oversees the implementation of the Information Sharing Environment across federal, state, local, tribal, and private sector boundaries.
- The Committee on National Security Systems (CNSS) provides a forum for the discussion of policy issues, and is responsible for setting national-level information security policies, directives, instructions, operational procedures, guidance, and advisories for federal agencies for the security of National Security Systems through the CNSS Issuance System.
- The Insider Threat Task Force (ITTF) is intended to integrate counterintelligence, personnel security, information security, human resources and other relevant functions, and disciplines to effectively counter insider threats, while promoting appropriate sharing and safeguarding of national security information consistent with civil liberties and privacy regulations.

Throughout 2012 the Steering Committee, ITTF, ISA-IPC, CNSS, and PM-ISE collaborated with Federal agencies on the following additional activities across classified and unclassified[16] exchange environments:

- Developed the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) which was issued by the President in November 2012.
    - The National Insider Threat Policy and Minimum Standards will strengthen the Federal Government safeguarding postures through viable and effective Threat Detection programs to enhance the protection of National Security Information.
- Assisted agencies to establish viable insider threat detection and prevention programs through periodic consultations and assistance visits.

[16] For unclassified systems, FISMA requires the head of each Federal agency to provide information security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency and information system used or operated by an agency or by a contractor of an agency or other organization on behalf of the agency. FISMA requires similar protections to be provided by the head of each Federal agency that is operating or exercising control over national security systems.

- Developed assessment procedures and, as directed by the Steering Committee, conducted on-site evaluations to determine the adequacy of department and agency insider threat programs to meet related policy and standards.
- Identified best practices from across the Federal Government that can be leveraged for shared services in the following areas: centralized incident reporting; online identity management; access control; and enterprise audit.

B. Supporting Safe and Secure Adoption of Emerging Technologies

The Federal Government is harnessing the transformative power of emerging technologies such as cloud computing, mobile computing and wireless platforms, applications and tools to efficiently and effectively provide the American people and Federal employees access to Federal information, services and resources when, where and how they want them. In order to seamlessly integrate these innovative solutions into government operations, we must minimize the inherent security risks associated with these technologies.

Facilitating Mobile Security

In May 2012, the President signed a Memorandum issuing the Digital Government Strategy, which was designed to build a 21st Century digital government that delivers better services to the American people. The strategy embraces the need to innovate and architect systems and services to leverage the unique capabilities of 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.

It is imperative that security, privacy, and data protection mechanisms be built in throughout the entire technology life cycle in order to promote greater information sharing and collaboration through the use of mobile technologies. To further this objective, NIST has issued a series of resources to assist organizations in managing challenges associated with increased use of mobile devices. In July 2012, NIST issued draft Special Publication 800-124 Revision 1; "Guidelines for Managing and Securing Mobile Devices in the Enterprise", to help organizations centrally manage and secure mobile devices (organization-provided and personally-owned) against a variety of threats. NIST also researched and issued draft Special Publication 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.

Much like mobile devices, mobile applications must also be managed and secured. Mobile devices are designed to make it easy to find, acquire, install, and use third-party applications. This poses security risks, especially for mobile device platforms that do not place security restrictions or other limitations on third-party applications. NIST has conducted research in new testing methodologies for mobile device apps and plans to release guidelines to provide a methodology for testing and vetting third-party applications that are distributed through various app stores.

The increased adoption and use of mobile devices and technologies, coupled with the continued implementation of various Federal telework initiatives, is enabling a growing and more efficient mobile workforce. Telework provides benefits beyond continuity of operations, such as in reducing transit subsidy and real estate costs. Implementing an effective telework strategy affects several

areas of consideration, such as human-capital policies and procedures, telecommunication infrastructure, and facility space utilization. As with any initiative, if telework is not properly implemented, it may also introduce new information security and privacy vulnerabilities into agency systems and networks.

In the coming year, NIST, working collaboratively with agencies and industry, plans to issue a series of publications that will assist agencies in securing their mobile device and telework implementations. NIST plans to issue draft Special Publication 800-157 that will provide technical specifications for the use of PIV derived credentials to enable authentication services for mobile devices that do not currently provide easy or practical support for smart cards. NIST also plans to issue draft Special Publication 800-114 Revision 1, "User's Guide to Telework and Bring Your Own Device (BYOD) Security", which will provide recommendations for securing BYOD devices used for telework and remote access, as well as those devices directly attached to the enterprise's own networks. In addition, NIST plans to release draft Special Publication 800-46 Revision 2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security", to provide information on security considerations for several types of remote access solutions, including recommendations for securing a variety of telework and remote access technologies.

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 "25 Point Plan to Reform Federal Information Technology Management".[17] The Federal Cloud Computing Strategy[18] identified ensuring the safety, security and reliability of data as an important challenge in moving to cloud computing environments. Recognizing this challenge, the Federal CIO published on December 8, 2011 the policy memo, "Security Authorization of Information Systems in Cloud Computing Environments". This memo formally established the Federal Risk and Authorization Management Program (FedRAMP) and set out roles and responsibilities, implementation timelines, and requirements for agency compliance.

The FedRAMP Program achieved its FY 2012 milestones in an effort to create a standard approach for conducting security assessments of cloud systems. Shortly after its launch, FedRAMP published a baseline set of security controls and developed a comprehensive concept of operations, conformity assessment process, and continuous monitoring framework for Federal agencies to use when leveraging FedRAMP. On June 6, 2012, FedRAMP launched Initial Operational Capability, and begin accepting applications from Cloud Service Providers. FedRAMP actively engaged public and private sector stakeholders to refine its processes, conducted informational sessions and specialized training, and prepared for the launch of Full Operational Capability in 2013. The program's FY 2012 achievements serve as a baseline for FedRAMP's future success and will accelerate the adoption of secure cloud solutions in government through the reuse of assessments and authorizations.

---

[17] Office of Management and Budget, U.S. Chief Information Officer, "25 Point Implementation Plan To Reform Federal Information Technology Management", Dec. 9, 2010 at: http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf

[18] Office of Management and Budget, U.S. Chief Information Officer, "Federal Cloud Computing Strategy", Feb. 8, 2011 at: http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

In support of the Federal cloud computing efforts, NIST developed a draft Federal Government cloud computing roadmap which contains the high-priority requirements regarding security, portability and interoperability needed to further USG cloud computing adoption, and provides useful information for cloud adopters. The purpose of the roadmap is to accelerate Federal agencies' adoption of cloud computing, support the private sector, improve information available to decision makers, and facilitate the continued development of the cloud computing model.

Additionally, NIST continues to collaborate with a broad group of Federal stakeholders to reach consensus on cloud security, portability and interoperability standardization priorities as GSA develops and makes secure government-wide cloud procurement vehicles available to agencies. Taken together, these initiatives, along with agency-specific efforts under FISMA, will ensure the Federal Government's shift to the cloud occurs in a secure and responsible manner.

Implementing Internet Protocol Version 6

In September 2010, OMB issued a memorandum[19] requiring Executive Branch agencies to operationally deploy native Internet Protocol Version 6 (IPv6) for public Internet servers and internal applications that communicate with public servers.[20] This directive builds upon an August 2005 memorandum[21], "Transition Planning for Internet Protocol Version 6 (IPv6)", which led to the key early step of IPv6 deployment in all Federal Government network backbones in 2008. IPv6 is expected to enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems.

It is essential that Federal agencies migrate to IPv6 to ensure continuity of operations; however, IPv6 will also lead to new challenges and types of threats facing an organization. To address these challenges, in July 2012, the Federal Government released a roadmap for transitioning to the next-generation Internet networking technology. This Roadmap, "The Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government" was jointly developed with the American Council for Technology – Industry Advisory Council (ACT-IAC) and provides best practices on how to successfully implement the next version of the Internet Protocol – IPv6. The IPv6 Roadmap, along with NIST Special Publication 800-119,[22] includes guidance for securely implementing IPv6 within the Federal enterprise.

National Strategy 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)[23] in April 2011. 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

---

[19] Memorandum dated Sept. 28, 2011. Subject: "Transition to Internet Protocol Version 6 (IPv6)". See: https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf.

[20] Agency status towards IPv6-enabling public Internet servers is available on the NIST IPv6 Deployment Monitor at: http://fedv6-deployment.antd.nist.gov/.

[21] Memorandum dated Aug. 5, 2005. Subject: "Transition Planning for Internet Protocol Version 6 (IPv6)". See: http://www.whitehouse.gov/ sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf.

[22] NIST Special Publication 800-119, Guidelines for the Secure Deployment of IPv6, was issued in December 2010 and can be accessed at: http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[23] Located at: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

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 ICAM roadmap discussed earlier 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 who will oversee a Federal Cloud Credential Exchange (FCCX) pilot in 2013. 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 the 21st Century Workforce

To protect and defend the nation's digital information and infrastructure, the United States must develop an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats. In the past, there has been little consistency in how the cybersecurity workforce and cybersecurity work is defined or described throughout the nation. The absence of a common language to discuss and understand the work and skill requirements of cybersecurity professionals has severely hindered our nation's ability to baseline capabilities, identify skill gaps, develop cybersecurity talent in the current workforce, and prepare the pipeline of future talent. Establishing and using a common lexicon and taxonomy for cybersecurity work and workers is not merely desirable, but critical to the nation's cybersecurity mission. Given these challenges, the following actions have been undertaken in 2012.

Established National Cybersecurity Workforce Framework

Defining the cybersecurity population consistently, and using standardized terms, is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. To meet this need, the "National Cybersecurity Workforce Framework" was finalized and approved by the Office of Management and Budget in September 2012 and published on the National Institute for Standards and Technology (NIST)'s National Initiative for Cybersecurity Education (NICE)[24] website at https://www.nist.gov/nice/framework. The Framework lists and defines 31 specialty areas of cybersecurity work and provides a description of each. Each of the types of work is placed into 1 of 7 overall categories. The Framework also identifies common tasks and Knowledge, Skills, and Abilities (KSAs) associated with each specialty area.

The Framework provides the groundwork, or a baseline, by which organizations can develop their Human Capital Management programs, including defining roles, designing competency models, standardizing job descriptions, and providing specialized training. The Framework will be used as guidance to the Federal Government. It will be made available to the private, public, and academic

[24] NICE is a Federal and nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Defining the cybersecurity population consistently, and using standardized terms, is an essential step in ensuring that the country is able to educate, recruit, train, develop, and retain a highly-qualified workforce.

sectors for describing cybersecurity work and workforces, and the related education, training, and professional development sectors.

The Framework was developed as a direct result from the White House's need to quickly identify, quantify, and develop an effective cybersecurity workforce to enhance our Nation's critical cyber infrastructure. The Framework reflects the collaborative efforts of over 20 Federal agencies and numerous national organizations from within academia and general industry.

Established Online Resources for Education and Awareness

The National Initiative for Cybersecurity Careers and Studies (NICCS) portal[25] , a public facing website, was developed by DHS to be an online resource for cybersecurity awareness, education, training, and career information. The vision of NICCS portal is to provide a national resource to elevate cybersecurity awareness and affect the change in the American public; to adopt a culture of cyberspace security and to build a competent cybersecurity workforce. The NICCS portal leverages the efforts of government, industry, and academia to provide a comprehensive, single source to address cybersecurity informational and needs. The portal also includes information researched and developed through NICE, DHS and other organizations in government, industry and academia as well as the initial efforts of the "Cybersecurity Training and Education Catalog", which will provide a robust and representative resource of available cybersecurity training that aligns to the specialty areas within the Framework.

Released Workforce Development Matrices

The Information Security and Identity Management Committee (ISIMC) and the IT Workforce Committee (ITWC) of the Federal CIO Council publicly released four Cybersecurity Workforce Development Matrices and the accompanying "Cybersecurity Workforce Development Matrix Resource Guide" in December 2011[26]. The matrices are intended to give Federal agencies a common framework for describing competencies/skills, education, experience, credentials and the training needed by performance level for each of the identified roles. The resource guide supports the initiative by providing agency personnel with a desktop reference for developing human capital and workforce development activities, with a particular focus on their Cybersecurity workforces. The NICE Career Roadmap was developed in conjunction with the Framework. All future updates to Cybersecurity roles and matrices will be based on both the Roadmap and the Framework. The "Information Technology Workforce Assessment for Cybersecurity" (ITWAC) was an ITWC and DHS partnership effort completed for federal agencies to further identify the composition and capabilities of the federal IT civilian workforce executing cybersecurity responsibilities. This assessment assists with:

- Identifying Federal employees with cybersecurity job responsibilities;
- Establishing a baseline of current cybersecurity capabilities and proficiencies among the Federal workforce; and
- Understanding the scope of the cybersecurity workforce pipeline.

[25] Located at: http://niccs.us-cert.gov

[26] Located at: http://www.cio.gov

Empowering a Mobile Workforce

The increased adoption and use of mobile devices and technologies, coupled with the continued implementation of various Federal telework initiatives, is enabling a growing and more efficient mobile workforce. Telework provides benefits beyond continuity of operations, such as in reducing transit subsidy and real estate costs. Implementing an effective telework strategy affects several areas of consideration, such as human-capital policies and procedures, telecommunication infrastructure, and facility space utilization. As with any initiative, if telework is not properly implemented, it may also introduce new information security and privacy vulnerabilities into agency systems and networks.

In the coming year, NIST, working collaboratively with agencies and industry, plans to issue a series of publications that will assist agencies in securing their mobile device and telework implementations. NIST plans to issue draft Special Publication 800-157 that will provide technical specifications for the use of PIV derived credentials to enable authentication services for mobile devices that do not currently provide easy or practical support for smart cards. NIST also plans to issue draft Special Publication 800-114 Revision 1, "User's Guide to Telework and Bring Your Own Device (BYOD) Security", which will provide recommendations for securing BYOD devices used for telework and remote access, as well as those devices directly attached to the enterprise's own networks. In addition, NIST plans to release draft Special Publication 800-46 Revision 2, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security", to provide information on security considerations for several types of remote access solutions, including recommendations for securing a variety of telework and remote access technologies.

D. Improving Cost Effectiveness

Strategic Sourcing

The Federal Government has moved to leverage its buying power to help agencies obtain the security tools they need. The Information Systems Security Line of Business (ISSLoB) is a cross-government strategic sourcing initiative that identifies common information security needs across the Federal Government and delivers product and service solutions to improve information security program performance, reduce overall costs, and increase efficiency and standardization across U.S. Federal, State, and local governments. ISSLoB delivers these solutions through the establishment of government Shared Service Centers (SSCs) and the establishment of government-wide acquisition vehicles in partnership with GSA.

In FY 2012, the ISSLoB continued promoting the use of the Situational Awareness Incident Response (SAIR) Tier I and RMF Blanket Purchase Agreements (BPAs). Federal agencies purchasing products off the BPAs realized an additional $14 million in cost avoidance versus standard GSA pricing for the same information security products. Additionally, the Shared Service Centers providing general Security Awareness Training (SAT) Tier I – excluding OPM, DOD, and VA – realized almost $9 million in cost avoidance and Authorization & Accreditation – excluding DOI National Business Center, Bureau of Public Debt, and DOJ - showed more than $5 million in cost avoidance when compared to GSA Schedule 70 pricing.

ISSLoB developed the requirements for Situational Awareness Incident Response (SAIR) Tier III Continuous Monitoring Tools, which have evolved into requirements supporting the DHS Continuous Diagnostics and Mitigation Program and will continue to work with its acquisition and

Federal civilian agency partners to continue examining opportunities for delivering an economical means to implement security capabilities across the Federal enterprise.

III. 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/Local governments, commercial enterprises, U.S. citizens and international Computer Security Incident Response Teams (CSIRTs).[27] The total number of incidents for each group can be found in Table 1 below.

Table 1. Incidents Reported to US-CERT in FY 2012

Reporting Source	Total Number of Incidents
Federal Government Total	48,842
Federal Government: CFO Act	46,043
Federal Government: Non-CFO Act	2,799
Other (State, Local, Tribal Governments and Commercial)	104,201
TOTAL	153,043

The total number of reported incidents impacting the Federal Government increased by approximately 5% from FY 2011 while the number of reported incidents from all sectors combined increased by approximately 42% for the same period.

- In FY 2011, US-CERT received a total of 107,655 reports, of which 43,889 of impacted Federal agencies. This includes both CFO Act and Non-CFO Act agencies.
- In FY 2012, US-CERT received a total of 153,043 reports, of which 46,043 of impacted CFO Act agencies and 2,799 impacted Non-CFO Act agencies.

For FY 2012, US-CERT processed 153,043 incidents as categorized in Figure 2.[28] Phishing, a type of social engineering which is reported voluntarily to US-CERT by private individuals and organizations, continues to be the most widely reported incident type. As indicated in Figure 2, which includes a breakout of all incidents reported to US-CERT in FY 2012, phishing accounted for 68.3% of total incidents reported. Definitions for all attributes are in Table 2.

[27] A computer security incident, as defined by NIST Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

[28] For more information, refer to the US-CERT website at: http://www.us-cert.gov/.

Figure 2. Summary of Total Incidents Reported to US-CERT in FY 2012

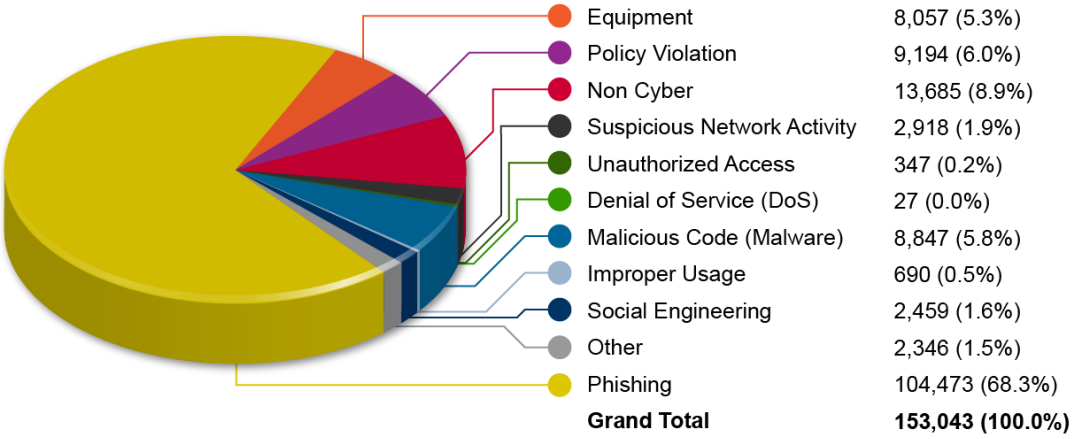
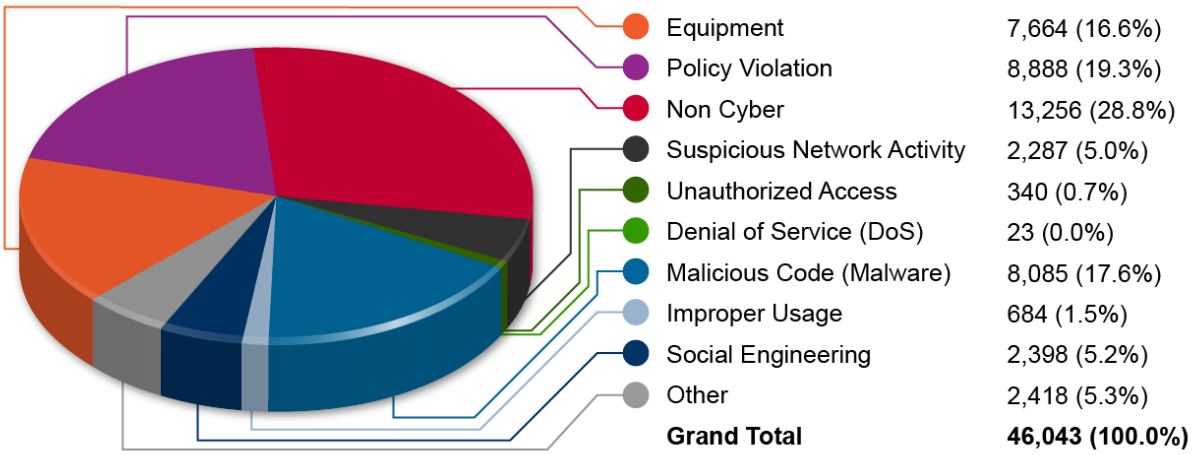


Table 2. US-CERT FY 2012 Incident Definitions

Category/Sub-Category	Usage
Unauthorized Access	Unauthorized Access is used to categorize all incidents where an unprivileged user gains or may have gained control of a system or resource. Equipment is a specific subset of this category.
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.
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.
Malicious Code	Used for all successful executions or installations of malicious software which are not immediately quarantined and cleaned by preventative measures such as anti-virus tools.
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.
Policy Violation	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.
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 Attempted Access.
Phishing	This is a specific subset of Attempted 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.
Suspicious Network Activity	This category is primarily utilized for incident reports and notifications created from EINSTEIN and EINSTEIN 2 data analyzed by US-CERT.
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.

During FY 2012, US-CERT processed 46,043 incidents reported by CFO Act agencies as categorized in Figure 3. A list of CFO Act agencies can be found in Appendix 5.

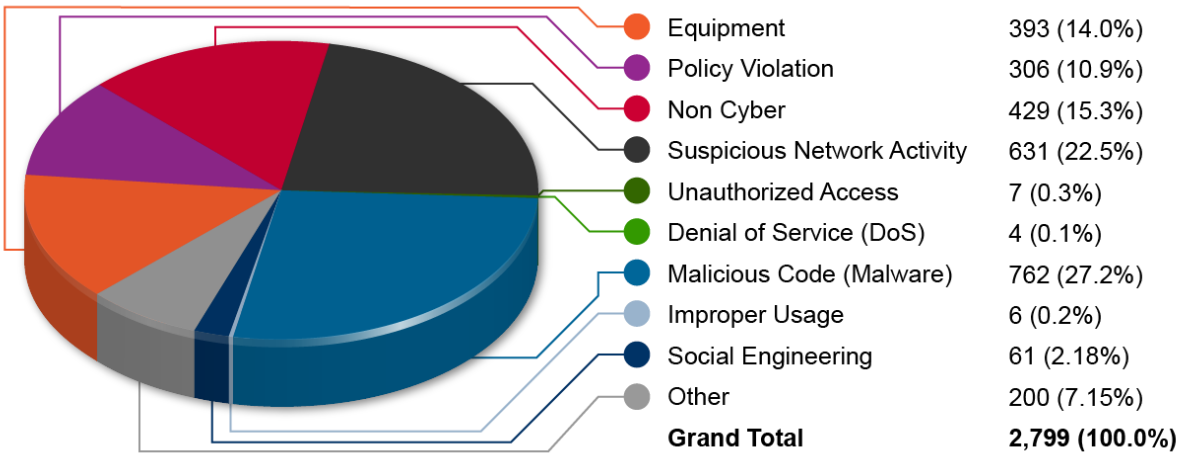
Figure 3. Summary of CFO Act Agency Incidents Reported to US-CERT in FY 2012



CFO Act agencies primarily reported incidents involving the loss or theft of IT equipment, such as laptops, mobile devices, authentication tokens or smart cards, and incidents involving the mishandling of potentially sensitive or controlled unclassified information. Where incidents involve the mishandling of sensitive information without a cybersecurity component, such as the loss of hard copy PII records, those are categorized as "Non Cyber" by US-CERT. For the first time, we have included detailed security incident information reported by agencies. A pie chart on security incidents reported by each CFO Act agency can be found in Appendix 2.

Federal agencies are not required to report attempted phishing incidents and primarily report incidents which involve the compromise of IT assets and/or spillage of sensitive information. During FY 2012, US-CERT processed 2,799 incidents reported by non-CFO Act agencies as categorized in Figure 4.

Figure 4. Summary of Non-CFO Act Agency Incidents Reported to US-CERT in FY 2012



Non-CFO Act agencies primarily reported incidents involving infections of malicious code 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.

The Federal Government continues taking significant measures to more accurately and efficiently identify and respond to security incidents when they occur. In FY 2012, US-CERT issued multiple products to Federal and private sector partners to promote information sharing and to help prevent and mitigate cyber attacks. These products (e.g., Early Warning and Indicator Notices (EWINs), Security Awareness Reports (SARs), and Department/Agency Cyber Activity Reports (DCARs) among others) often included information gathered through analysis of suspicious traffic detected via the Einstein system.

US-CERT releases EWINs to notify agencies and partner organizations of malicious activities. EWINs provide indicators for administrators to prevent or identify infections in their systems. US-CERT also provided mitigation steps with SARs and followed up with impacted agencies.

In addition to EWINs, US-CERT issues weekly DCARs to detail and document cybersecurity trends observed in the .gov domain for senior cybersecurity leaders in the Federal Government. US-CERT compiles weekly data generated through analysis of agency reporting and Einstein activity, which provides context for the common threats to Federal stakeholders, as well as agency-specific data for some agencies. Beyond the 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 (ISC-CERT), and NCC among other organizations. US-CERT's collaboration with aforementioned entities has generated new lines of products such as the Joint Indicator Bulletin (JIB) and the Joint Security Awareness Report (JSAR).

The Federal Government continued to sponsor research and development of an insider threat assessment methodology and corresponding mitigation strategies through the CERT Insider Threat Center. This 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 that build one upon the other. The CERT Insider Threat Center has accelerated, and will facilitate, the identification and adoption of future insider threat controls through FISMA.

IV. Key Security Metrics

In FY 2010, FISMA reporting began the evolution from a compliance driven security focus to a performance and outcome based focus. The information security metrics are designed to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels. The FY 2012 FISMA metrics were developed through a collaborative effort from DHS, the Federal CIO Council, and several other organizations and working groups. The new baseline established in FY 2012 will continue to allow 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, and summary metrics data reported by non-CFO Act agencies.

Additionally, CFO Act agencies reported detailed security cost information through their Exhibit 53B submissions as part of their budget submissions to OMB. Information reported by the agencies included personnel costs for government and contractor resources, tool costs, testing costs, training costs, and costs for Risk Management activities (as required by NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*).

A. Information Security Metrics for CFO Act Agencies

The following sections highlight the FISMA metrics for the Cross Agency Priority Goals discussed in Section II, as well as other key FISMA metrics for FY 2012. All data are as reported by agencies with the exception of Domain Name System Security Extensions (DNSSEC) data which are validated values obtained through compliance scans and on-site assessments conducted by DHS.

Table 3 below provides a comparison of FISMA capabilities from FY 2011 to FY 2012. More specific information on each of these metrics is outlined in this section.

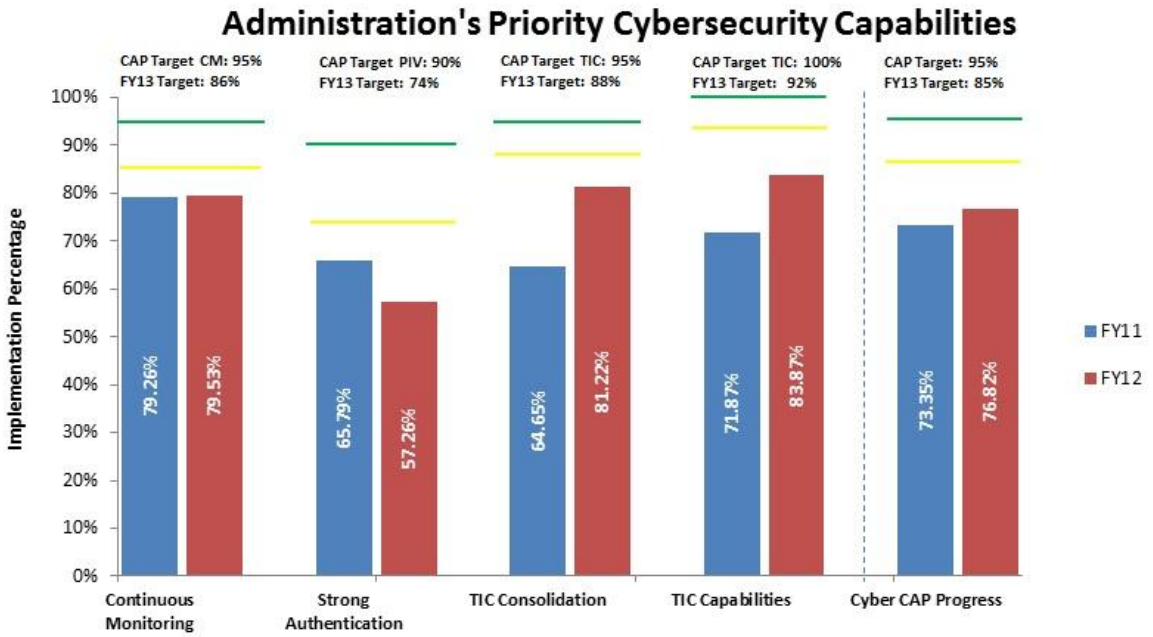
Table 3. Comparison of FISMA Capabilities from FY 2011 to FY 2012

Capability Area	FY 2011	FY 2012
Automated Asset Management	80%	86%
Automated Configuration Management	78%	70%
Automated Vulnerability Management	80%	83%
TIC Traffic Consolidation	65%	81%
TIC 1.0 Capabilities (Includes Einstein 2)	72%	84%
PIV Logical Access (HSPD-12)	66%	57%
Portable Device Encryption	83%	90%
DNSSEC Implementation	65%	74%
E-Mail Validation Technology	58%	64%
Remote Access Authentication	52%	53%
Remote Access Encryption	83%	82%
Controlled Incident Detection	49%	63%
US-CERT SAR Remediation	97%	96%
User Training	99%	88%
Users with Security Responsibility Training	92%	92%
Detect and Block Unauthorized Software	n/a	60%
Email Encryption	n/a	35%
Government-Wide Average	**75%**	**74%**

NOTE: Email Encryption and Detect and Block Unauthorized Software were not measured until FY 2012.

These metrics are also used to track progress against the CAP goals (TIC security capabilities and traffic consolidation; continuous monitoring; and HSPD-12 implementation for logical access). Overall, CAP goals have shown an overall improvement from 73% in FY 2011 to 77% in FY 2012. Progress against CAP goals is provided in Figure 5.

Figure 5. Percentage Implementation of Administration FISMA Priorities in FY2011 and FY2012



Note:

- Continuous Monitoring is comprised of the following capability areas: Automated Asset Management, Automated Configuration Management, and Automated Vulnerability Management.
- Strong Authentication is comprised of the PIV Logical Access (HSPD-12) capability area.
- TIC Consolidation is comprised of the capability area TIC Traffic Consolidation.
- TIC Capabilities is comprised of the capability area TIC 1.0 Capabilities (Includes Einstein 2).
- Cyber CAP Progress represents an average of: Continuous Monitoring, Strong Authentication, TIC Consolidation and TIC Capabilities.

Continuous Monitoring

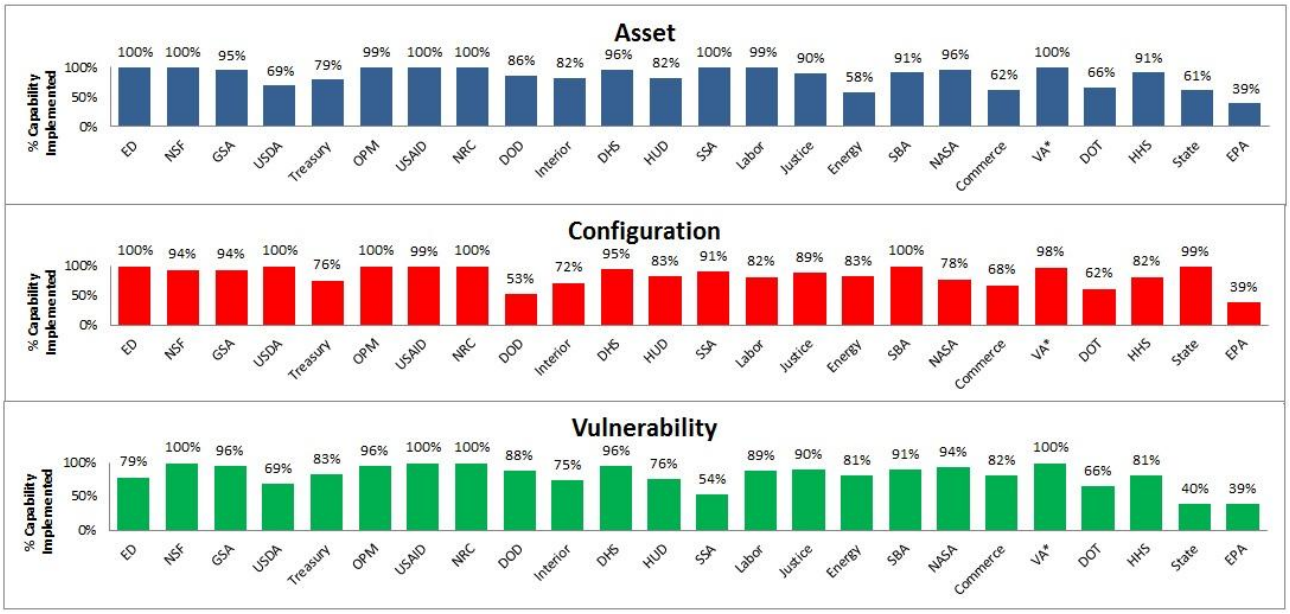
The increased adoption of continuous monitoring will ensure greater security through constant review. Recognizing the value of and need to incorporate feedback and improvements from other agencies, the Executive Office of the President has designated the Joint Continuous Monitoring Working Group (CMWG)[29] as the forum for interagency continuous monitoring program coordination. This group has determined that asset management, configuration management, and vulnerability management are the first areas where continuous monitoring needs to be developed. The three required data feeds to CyberScope (i.e., IT asset inventory, system configuration, and vulnerability management) have provided insight into the number of systems that are being managed under automated asset, configuration, and vulnerability management.

In FY 2012, all CFO Act agencies have shown the ability to successfully submit automated data feeds to CyberScope. Figure 6 illustrates the percentage of IT assets with automated access to asset

[29] The Federal CIO Council Information Security and Identity Management Committee (ISIMC) Continuous Monitoring Working Group (CMWG) and the Committee on National Security Systems (CNSS) CMWG are jointly referred to as the "Joint CMWG".

inventory, configuration management, and vulnerability management information by agency. In FY 2012, agency implementation of automated continuous monitoring capabilities increased slightly to 80% as compared to 79% in FY 2011.

Figure 6. Percentage of Continuous Monitoring Capabilities Reported by Agencies



*Note: VA's status represents a subset of their assets.

Although there was significant progress in asset and vulnerability management, this was outweighed by a substantial decline in configuration management. This is in part due to the fact that DOD decreased from 95% in FY 2011 to 53% in FY 2012 which is a result of the change in reporting criteria for the Configuration Management metric. This caused the government-wide average for continuous monitoring to decline. Other agencies, including the Office of Personnel Management, United States Agency for International Development, Department of Homeland Security, and Small Business Administration raised their continuous monitoring score by more than 35% from FY 2011 to FY 2012.

The goal of asset inventory management capability is to be able to account for 100% of agency's IT assets using an automated asset management system and to identify and remove unmanaged assets before they are exploited and used to attack other assets. In FY 2011, agencies reported automated inventory capturing with a success rate of 80%, but in FY 2012 the success rate increased to 86%.

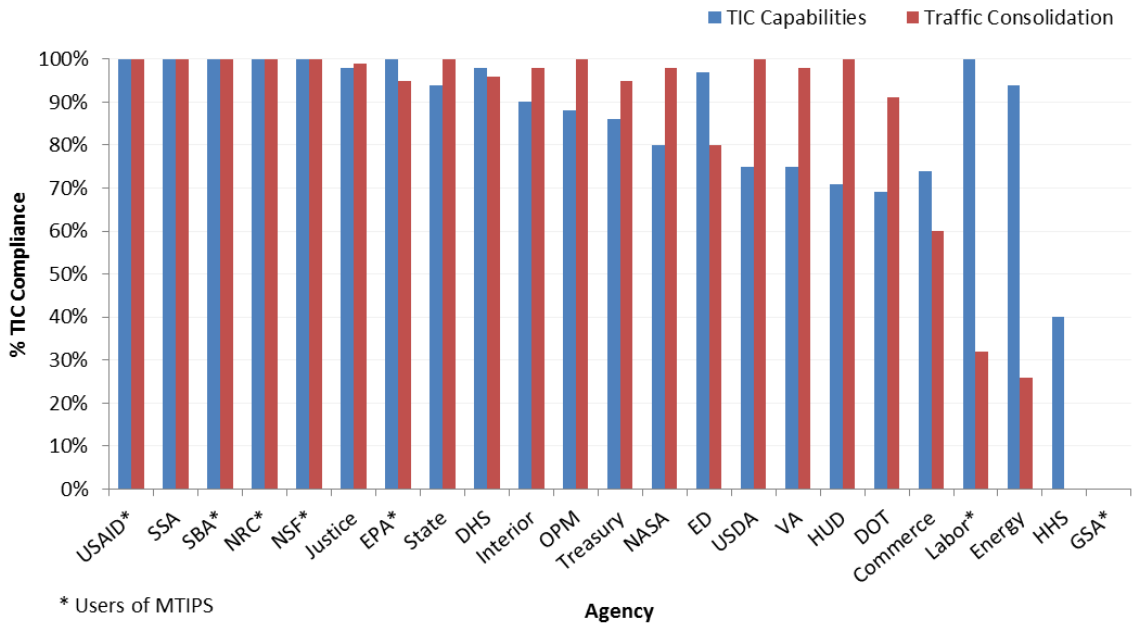
Improved configuration management and the development of secure configuration baselines allow for the operating system to be hardened, making it more difficult for attackers to exploit any vulnerabilities. All but one agency (i.e., USAID) reported that secure baselines had been defined for each operating system installed and in use on its assets. For system configuration, automated tools were used to keep track and compare agencies' information system baseline configurations to installed configurations in an effort to maintain consistent baselines and remediate non-compliant baseline configurations for all information systems. In FY 2011, agencies reported that the automated configuration management capability was 78%, and this level decreased to 70% in FY 2012.

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. In FY 2011, 80% of assets were being managed with an automated vulnerability management capability. At present, analysis of the vulnerability management capability across the government shows 83% of assets are being managed with an automated vulnerability management capability. A key goal of configuration and vulnerability management is to make assets more difficult to exploit by following published guidelines and best practices.

Trusted Internet Connections (TIC)

The TIC, a front line of defense for agencies, continued to make progress by the adoption of trusted providers for external telecommunications access points. Nineteen agencies are TIC Access Providers (TICAPS) and are responsible for managing a TIC and the attendant requirements. Four vendors have been designated to provide Managed Trusted Internet Protocol Services (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 51 critical security requirements that comprise the *TIC Reference Architecture Version 1.0* capability and for the percentage of their external network traffic passing through a TIC MTIPS vendor. The consolidation of external network traffic increased from 65% in FY 2011 to 81% in FY 2012 for the 24 CFO agencies (excepting DOD). The implementation of *TIC Reference Architecture Version 1.0* critical security capabilities also increased from 72% in FY 2011 to 84% in FY 2012. Figure 7 illustrates percentage of TIC security capabilities and traffic consolidation as implemented by agencies.

Figure 7. Percentage of TIC Security Capabilities and Traffic Consolidation Implemented by Agencies

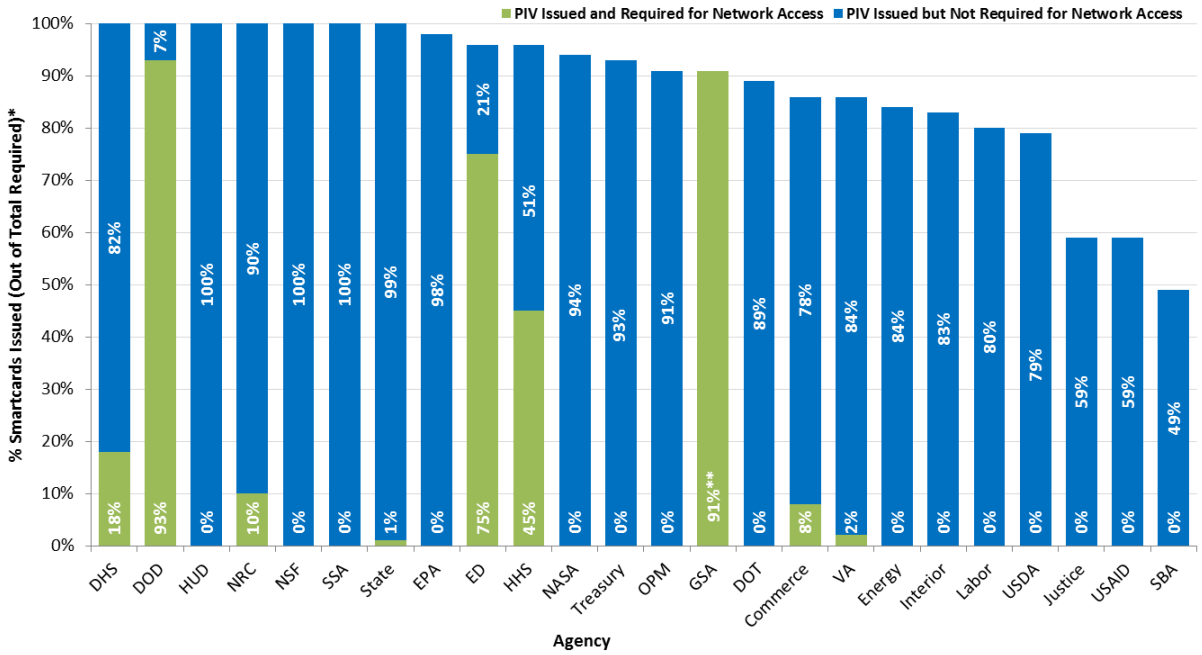


Strong Authentication: HSPD-12

In February 2011, OMB and DHS issued Memorandum M-11-11 directing agencies to issue policy and formulate an action plan for the full implementation of HSPD-12. As of September 1, 2012, 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 (smartcard) and something you know (PIN), reducing the risk of the assertion of a false identity. Figure 8 shows, by agency, the issuance progress and percentage of user accounts that require PIV cards for access to the agency's networks.

The FY 2012 FISMA metrics data indicates that 57% of government user accounts are configured to require PIV cards to authenticate to agencies' networks, down from 66% in FY 2011. A decrease at DOD and a significant decrease at USDA impacted the overall average. However, GSA, Education and Health and Human Services (HHS) reported significant increases. At this time last year, six agencies reported that 5% or more of user accounts required PIV cards for authentication, with four of those agencies at 44% or better. In FY 2012, mandatory PIV use increased to seven agencies reporting 8% or better and again four agencies reporting 45% or better. Of the remaining 17 agencies, two reported between 1% and 2% of employees were required to use their PIV cards to authenticate to the agency network, and 15 reported 0%.

Figure 8. Smartcard Issuance Progress and Percentage of User Accounts that Require the Use of PIV Cards for Network Access Reported by Agencies

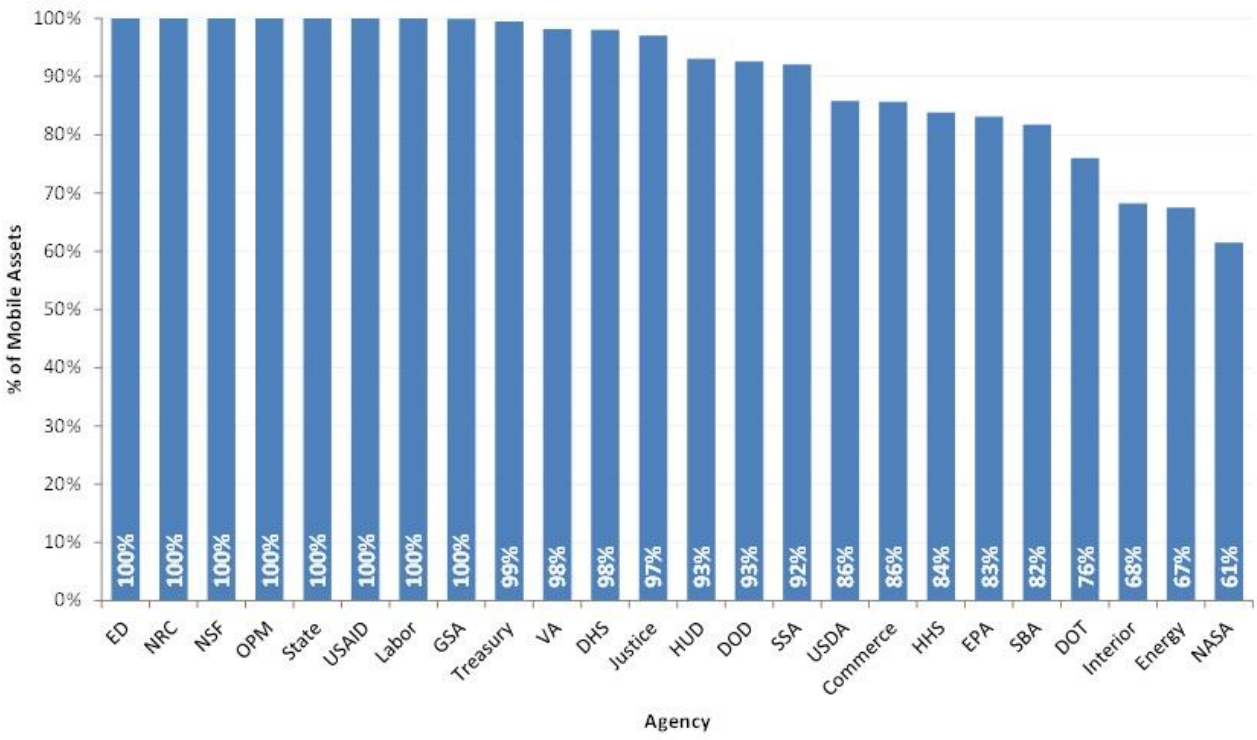


*All PIV card issuance percentages are from September 2012, and PIV card usage percentages are from November 2012
**GSA reported 79% PIV card issuance and 92% PIV card usage for network access

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. The ultimate goal is to have 100% of all portable computing devices encrypted with Federal Information Processing Standards (FIPS) 140-2 validated encryption, per M-06-16[30]. Similar to last year's metric, FY 2012 captured the encryption percentage of all mobile assets to include laptops, netbooks, tablet-type computers, Blackberries, personal digital assistants, smartphones, Universal Serial Bus (USB) devices and other mobile hardware assets. In FY 2012, agencies have reported continued progress in implementing this capability. In FY 2011 the reported government-wide average was 83%, but in FY 2012 the government-wide average is 90% with a third of the agencies achieving 100% encryption. 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 are also vectors to carry malware back into the intranet environment. The use of encryption of data at rest and/or in motion is vital to protect that data's confidentiality, integrity and/or availability. Figure 9 shows the percentage of agency portable devices with FIPS 140-2[31] validated encryption.

Figure 9. Percentage of Portable Devices with Encryption Reported by Agencies



[30] For details, see: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf

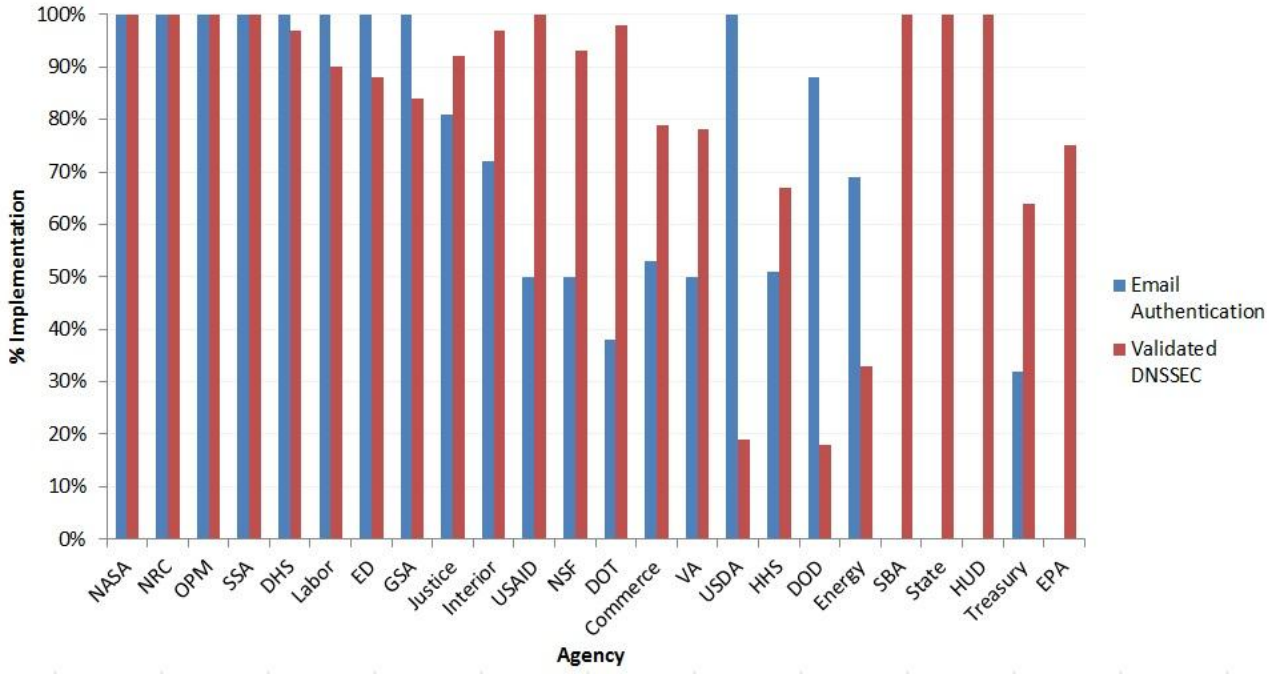
[31] NIST FIPS 140-2, "Security Requirements for Cryptographic Modules", located at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

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

Domain Name System Security Extension (DNSSEC) provides cryptographic protections to DNS communication exchanges, 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 has been mandated at the Federal level to prevent the pirating of government domain names. 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. Eight agencies, Department of Housing and Urban Development, United States Agency for International Development, National Air and Space Administration, Office of Personnel Management, Nuclear Regulatory Commission, Social Security Administration, Department of State, and Small Business Administration were validated as having 100% signed second level domains for DNSSEC.

Progress was reported from FY 2011 to FY 2012 in this capability area, with the government-wide compliance rate at 65% in FY 2011 to 74% in FY 2012 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. Organizations are expected to use these tools to measure compliance for their FISMA reporting. DHS also uses those tools to verify agency self-reported results. In the past, the results have indicated considerable deviation between the self-reported results and the DHS verification results. Organizations are expected to be more aware of the DNSSEC status when reporting and should be aware that a key reason for DNSSEC compliance problems in the past has been expiring certificates which are not updated by the owning Organization. Figure 10 shows by agency the DNSSEC deployment and percentage of email systems with sender verification technologies.

Figure 10. Percentage of Validated DNSSEC and Email Sender Verification Reported by Agencies



The 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 and arrive intact. A key objective is to increase the level of trust in email authenticity. In addition, fraudulent email sent to Federal agencies is a significant security risk for Federal systems. Email protections are directed to reduce the number of phishing attacks, which currently represent a high risk threat. By coupling anti-spoofing technologies with sender verification techniques, the security of email can be improved. In FY 2012, agencies were asked to report the percentage of agency email systems that implemented sender verification (anti-spoofing) technologies when sending messages and checked sender verification when receiving messages from outside the network. In FY 2011, the CFO Act agency average was reported at 58% for email validation. The CFO Act agency average has increased modestly to 64% in FY 2012 with a full third of the agencies are now achieving 100%.

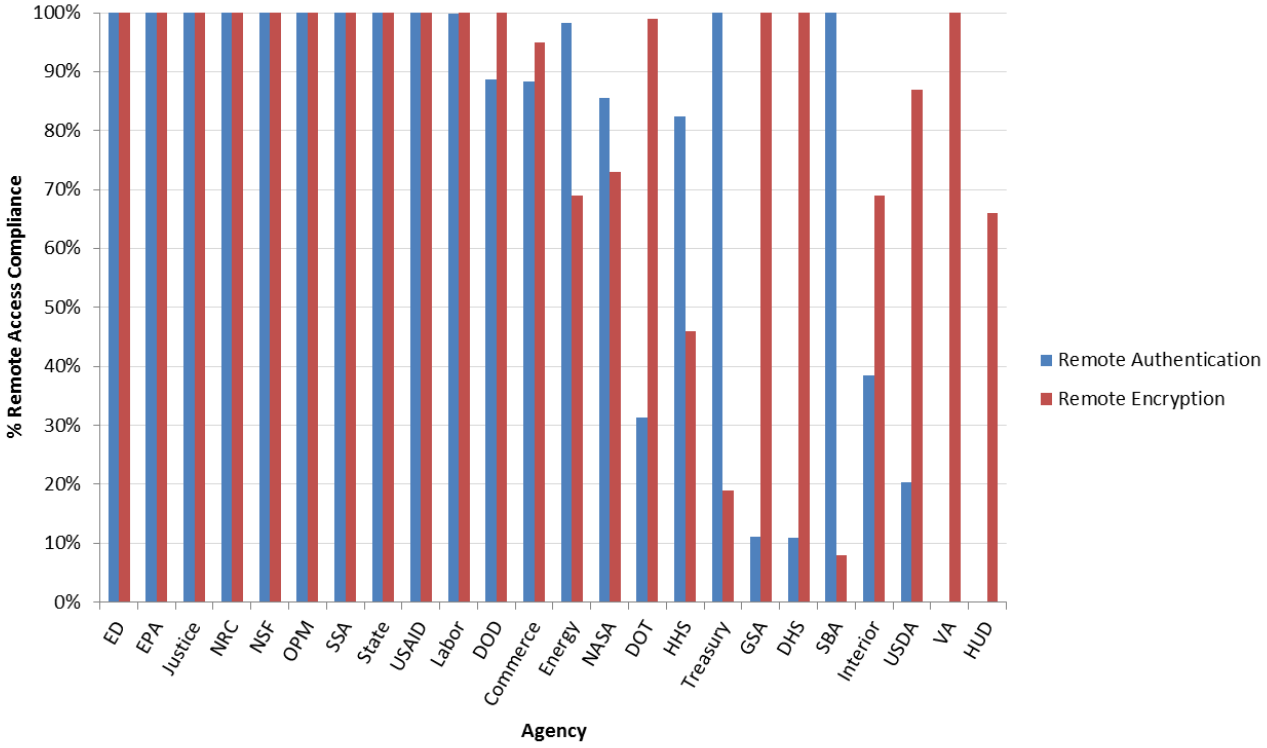
Remote Access

As the Federal Government promotes telework and increases their mobile workforce, remote access to network resources must require stronger authentication mechanisms than userID and password. Agencies were asked to report the total number of agency remote access connections and the number of those connections that required only userID and password as the sole method of authentication. Almost half the agencies have totally eliminated userID and password methods of access but there are still a couple of agencies that use this method for most, if not all, of their remote access connections. Across the government, 53% of remote access connections disallow the use of userID and password combinations as a method of authentication, basically consistent with FY 2011. Agencies were asked how many of their remote access connections utilized FIPS 140-2 validated cryptographic modules. FIPS 140-2 specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. In FY 2011, agencies responded that 83% of their methods of remote access utilized encryption but it was unknown how much each method was used. In 2012, remote access encryption was utilized on 82% of the actual remote connections for CFO agencies. More than half of the agencies reported 100% remote access encryption.

Adequate control of remote connections is a critical part of boundary protection. Remote connections allow users to access the network without gaining physical access to organization space and the computers hosted there. Moreover, the connections over the Internet provide opportunities for compromise of information in transit. Because these connections are beyond physical security controls, they need compensating controls to ensure that only properly identified and authenticated users gain access, and that the connections prevent hijacking by others. Attackers exploit boundary systems on Internet-accessible DMZ networks (and on internal network boundaries), and then pivot to gain deeper access on internal networks. Agencies must deter, detect, and defend against unauthorized network connections/access to internal and external networks. To assist agencies in securely implementing a telework infrastructure and ensuring that those infrastructures comply with Federal cybersecurity requirements, in FY 2012 DHS, in a multi-agency collaborative effort, published the "Telework Infrastructure Security Reference Architecture"[32]. Figure 11 shows the percentage of remote access connections, by agency, that require more than just userID and password authentication in addition to requiring FIPS 140-2 encryption for connections.

[32] Located at: http://www.dhs.gov/sites/default/files/publications/telework_reference_architecture-v1_0.pdf

Figure 11. Percentage of Remote Access Methods Disallowing UserID and Password for Authentication and Requiring Remote Access Encryption Reported by Agencies



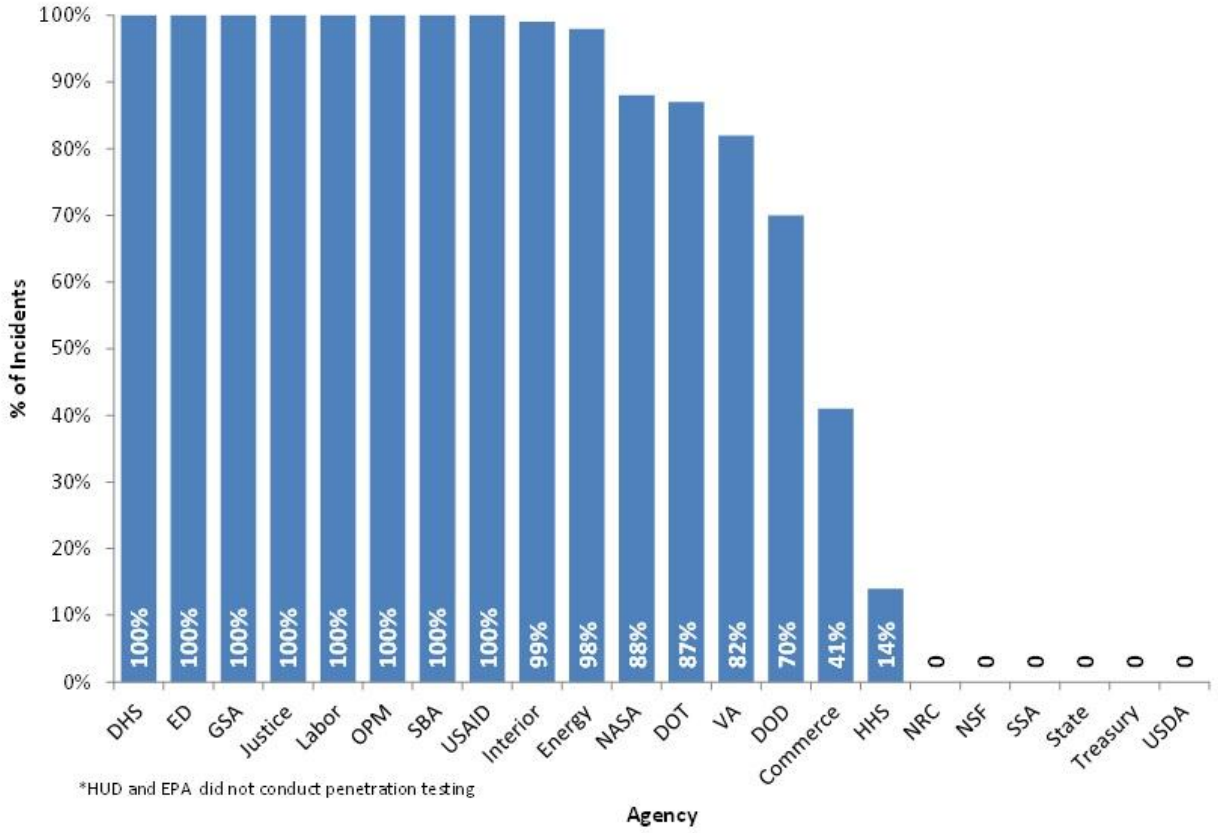
Controlled Incident Detection

The incident management capability must be coupled with a highly skilled and trained set of technical resources. 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 twenty two CFO Act agencies conducting controlled penetration tests, on average the NOC/SOC was 63% effective at detecting incidents, with 45% of the CFO Act agencies reporting a detection rate of 98% or better. This overall capability increased from 49% in FY 2011. Figure 12 illustrates the percentage of controlled penetration testing events detected by agencies.

Figure 12. Percentage of Controlled Incident Detection as Reported by Agencies



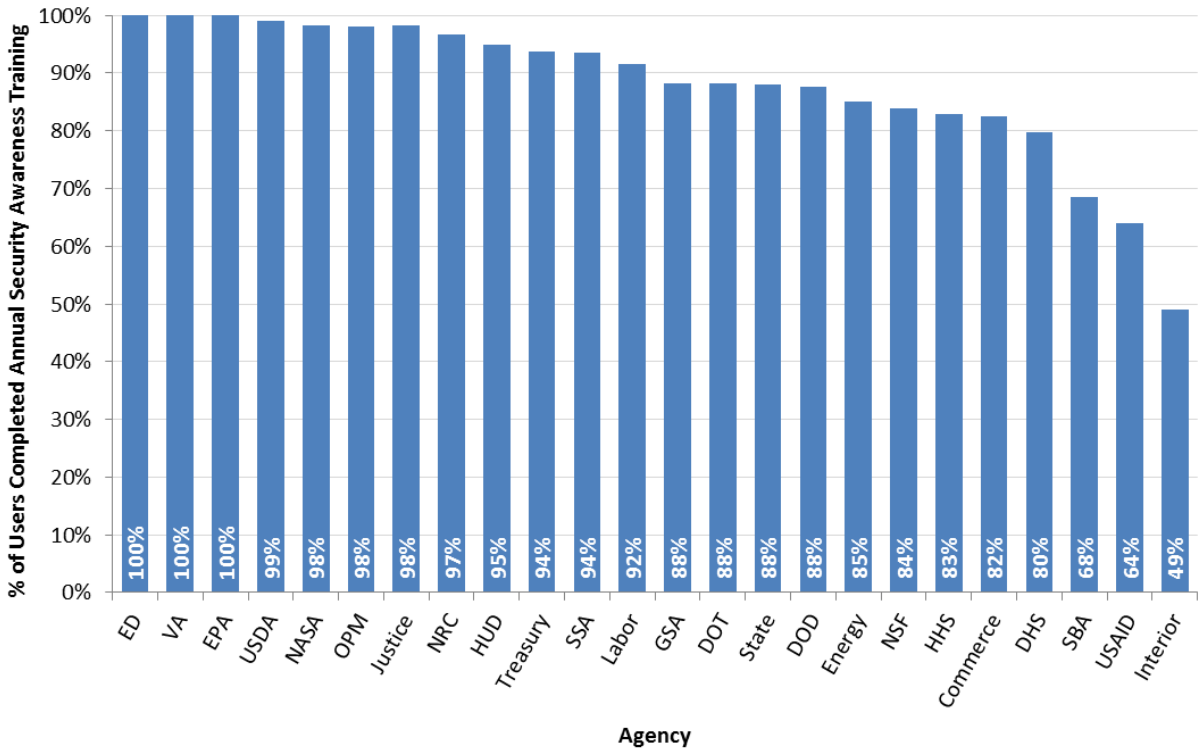
Security Training

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 (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, agencies are expected to use risk-based analysis to determine the correct amount, content, and frequency of update to achieve adequate security in the area of influencing these human behaviors that affect cybersecurity. The FY 2012, metrics were used to assess the extent to which agencies are providing adequate training to address these attacks and threats.

Agencies updated the content of their security training with greater frequency in FY 2012 and 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.

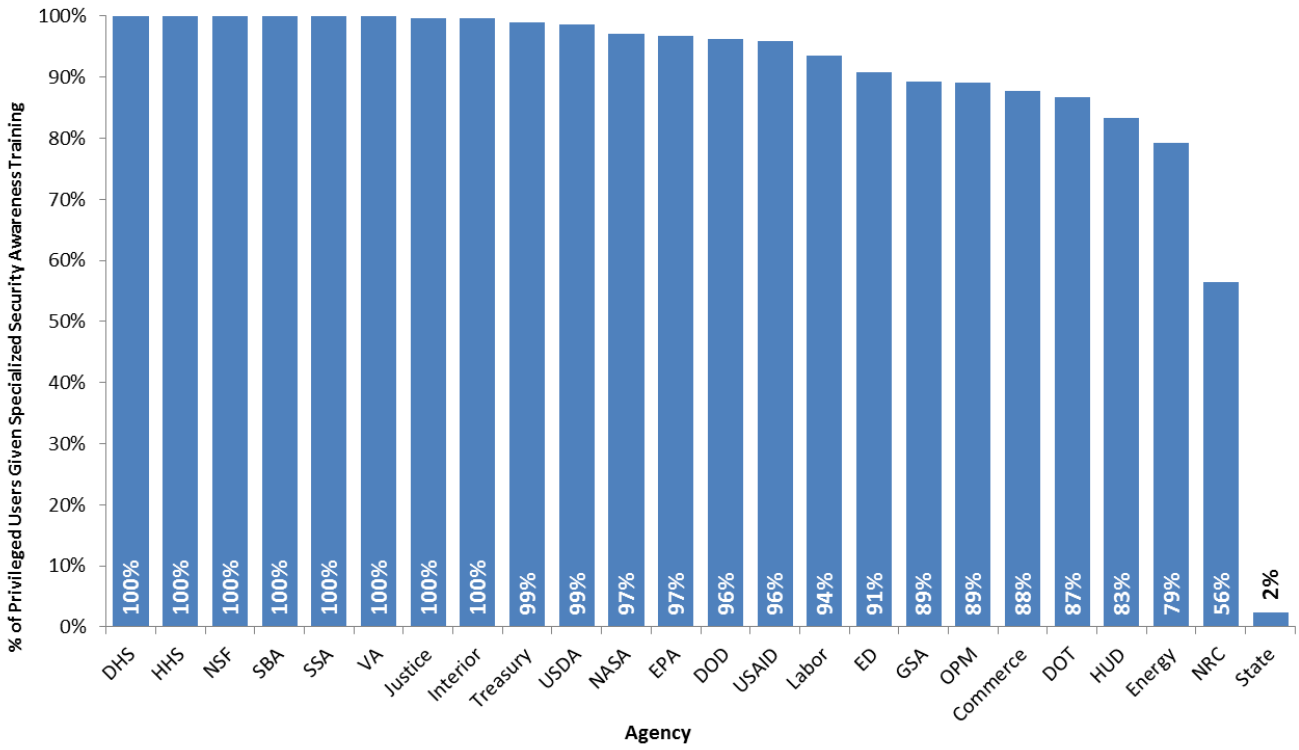
For agency users with network access privileges, 88% were given annual security awareness training, which is down from 99% in FY 2011. Agencies also reported that 89% of new users were given security awareness training prior to being granted network access, up from 83% in FY 2011. Figure 13 below provides by agency, the percentage of users completing annual security awareness training.

Figure 13. Percentage of Users with Network Access Completing Annual Security Awareness Training Reported by Agencies



Certain users have significant security responsibilities, a role where the daily assigned duties reflect an elevated authorized access to systems, data, and environments. This includes all users with privileged network user account(s) and all other users who have managerial or operational responsibilities that allow them to increase or decrease cyber security. After receiving the training, the user should be able to practice good behaviors and act wisely and cautiously, where judgment is needed, 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 to the extent 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 Federal agencies in FY 2012, the same as in FY 2011. Figure 14 below provides by agency, the percentage of agency users with significant security responsibilities given specialized annual cybersecurity training.

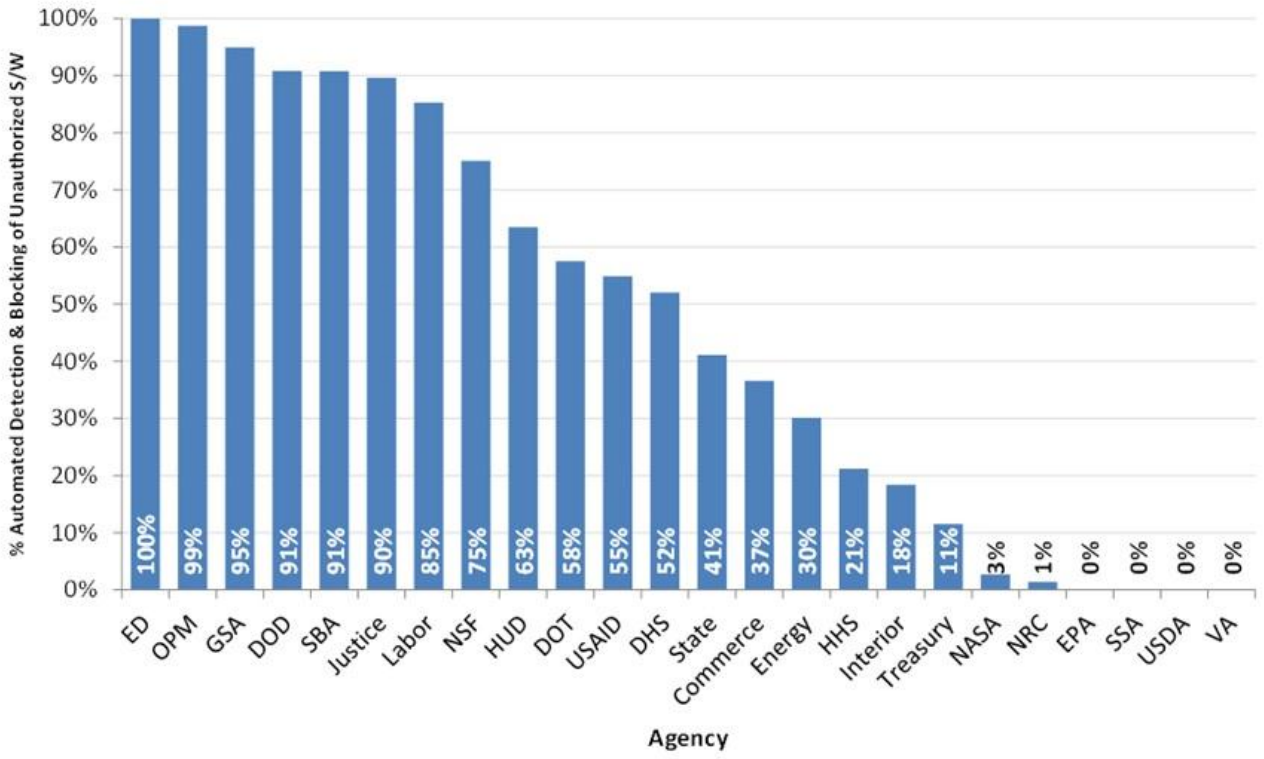
Figure 14. Percentage of Users with Significant Security Responsibilities Given Specialized Security Training Reported by Agencies



Automated Detection and Blocking of Unauthorized Software

Agencies were asked the number of assets where 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 60% of assets were covered by this capability with four agencies reporting 0% of assets covered. See Figure 15 below.

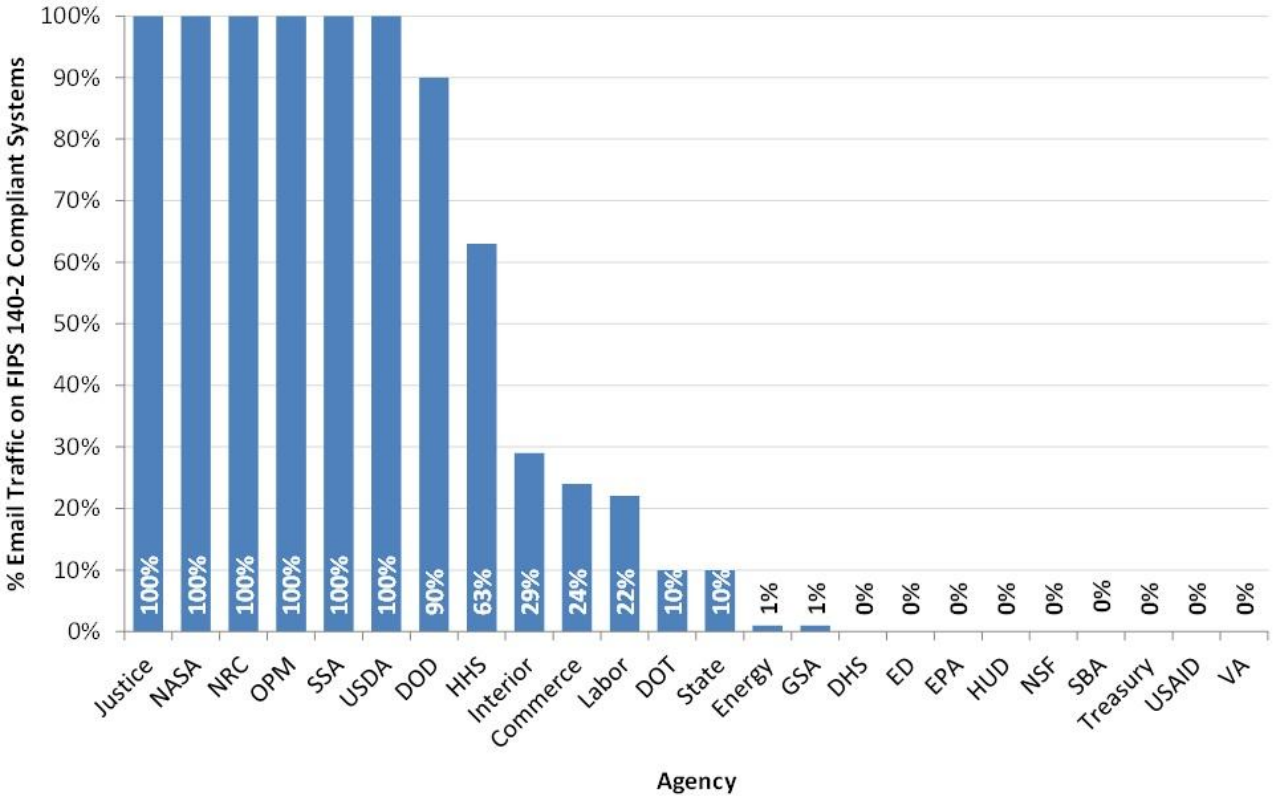
Figure 15. Percentage of Assets with Automated Capability to Detect and Block Unauthorized Software from Executing



Email Encryption

Unencrypted e-mails are a primary source of loss for sensitive data because they move outside the protection of physical and electronic barriers that protect other hardware assets. These devices are also vectors to carry malware back into the agency network environment. The use of encryption of data at rest or in motion is vital to protect that data's confidentiality, integrity and/or availability. Agencies were asked to provide the percentage of organization email traffic on systems that implement 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). Across the government, 35% of email traffic occurred on systems with encryption technologies. See Figure 16 below for more details.

Figure 16. Percentage of Email Traffic on Systems that Implement FIPS-140-2 Compliant Encryption technologies



B. Information Security Cost Metrics for CFO Act Agencies

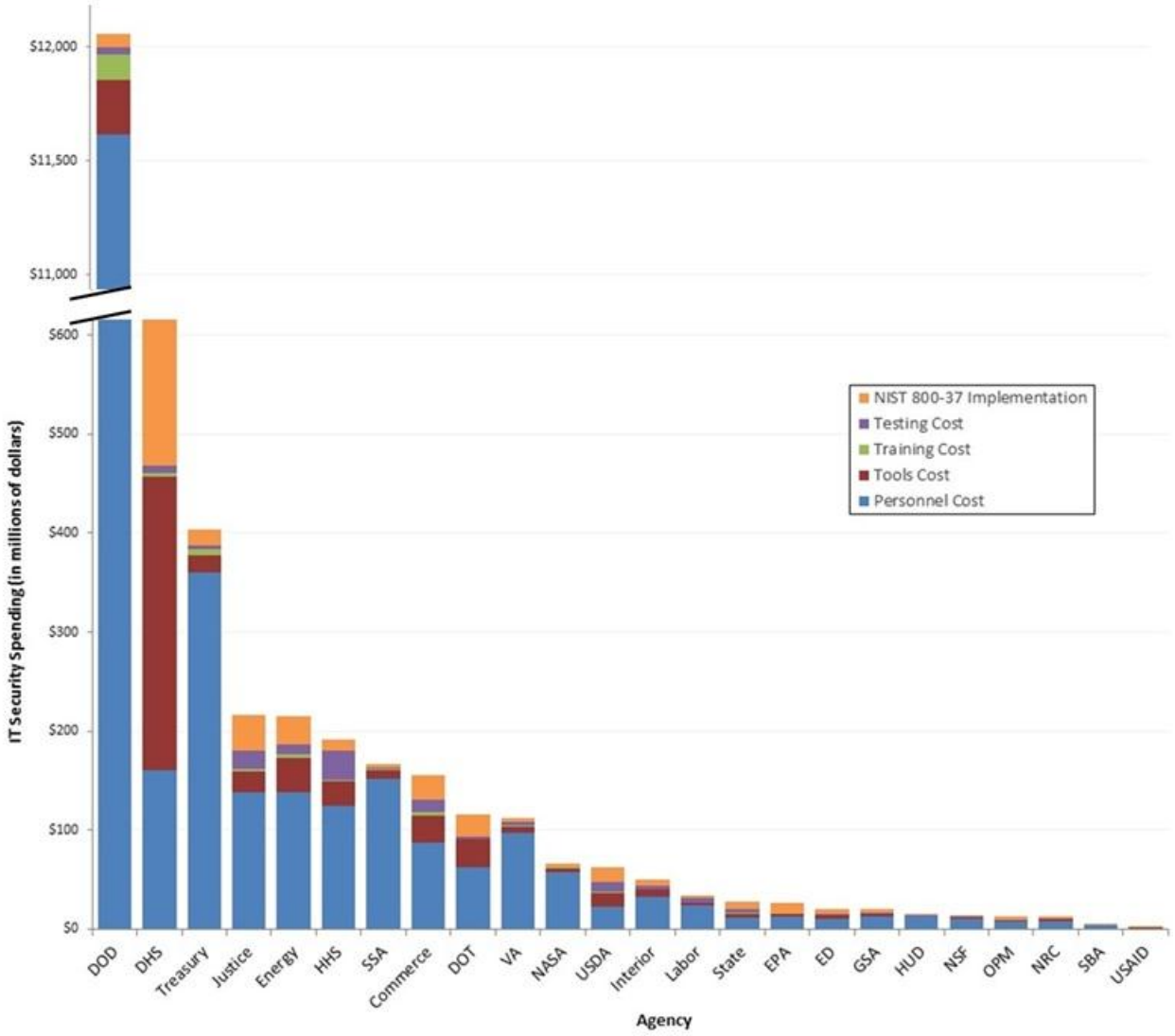
Sufficient resources must be devoted to ensure that the government's information and information systems that government and citizens' information remain secure. The OMB Exhibit 53B Agency IT Security Portfolio section[33] requires agencies to report IT security cost and budget data. All CFO Act agencies reported cost information in key areas including IT security testing, security tools, assessment and authorization, training, and personnel. This section of the FISMA report provides the IT security cost analysis based on the Exhibit 53B data for FY 2012.

IT Security Spending by Agency

In FY 2012, the CFO Act agencies, reported total IT security spending of $14.6 billion. Figure 17 provides the agency-reported IT security cost by spending category. Additional details on the personnel costs and specific cost values for each CFO Act agency can be found in Appendix 3: IT Security Spending Reported by Agencies.

[33] For more information, refer to:
http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy14_guidance_on_exhibits_53_and_300.pdf

Figure 17. IT Security Spending Reported by Agencies



IT security spending can be either direct or indirect:

- **Direct spending –** includes spending on items and activities such as security personnel, tools, testing, training, and risk management activities (i.e., NIST SP 800-37[34] implementation).

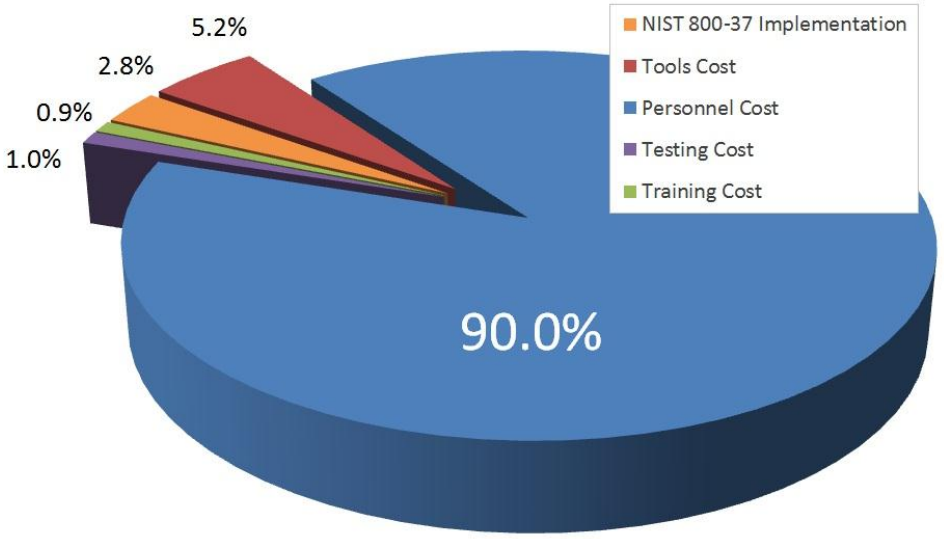
- **Indirect spending –** includes spending on items and activities such as security configuration fixes and recovering a compromised system; architecture redesign to enhance security; upgrading existing systems and installing replacement systems that provide more secure capabilities; institutionalizing IT security; and reporting and auditing.

[34] NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, at: http://csrc.nist.gov/publications/PubsSPs.html. This publication provides guidelines for applying the Risk Management Framework to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

The total IT security cost as reported by agencies is intended to capture costs for direct spending. However, the indirect costs of IT security can be difficult to separate from other operational and managerial costs. For instance, effective security programs are typically tightly integrated with other activities. Therefore, the total IT security cost reported may also include indirect spending.

In FY 2012, the bulk of agency-reported IT security spending government-wide was on personnel costs, which included salaries and benefits of government employees and the costs of contractors. CFO Act agencies spent 90% of their IT security costs on personnel, as indicated in Figure 18 below.

Figure 18. Percentage Breakout of IT Security Costs by Category Reported by Agencies



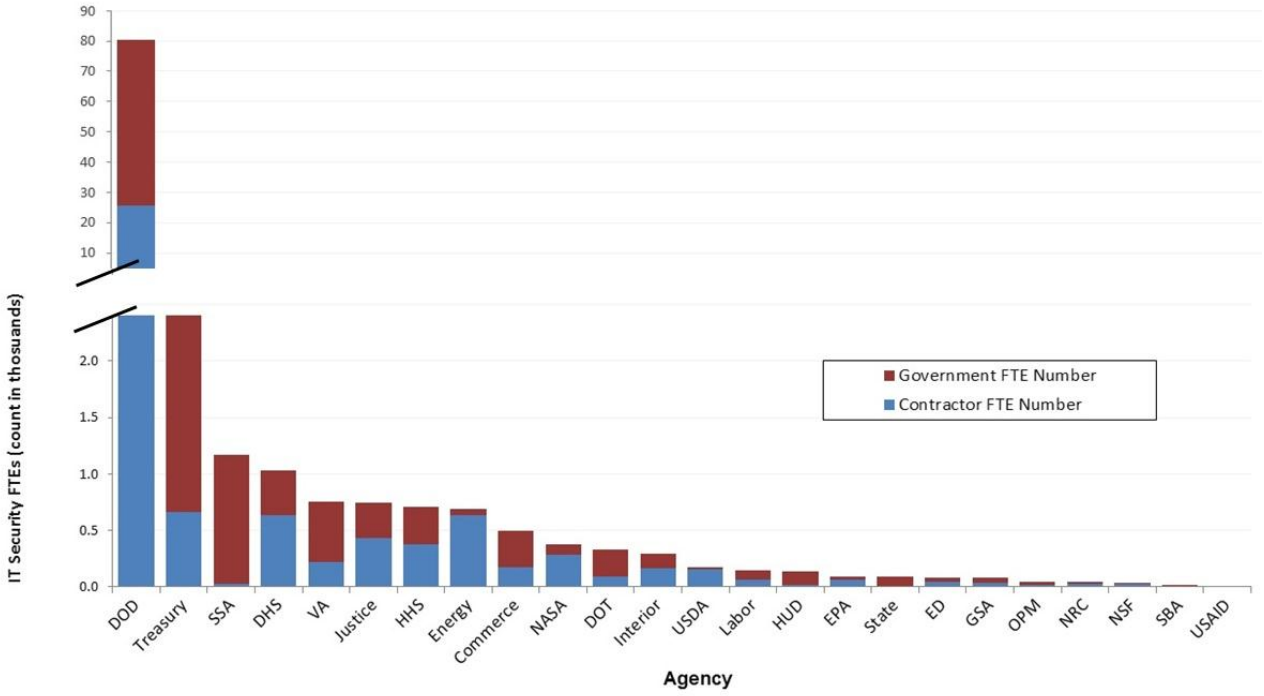
As further indicated by Figure 18 of the reported IT security costs government-wide, agencies spent 5% on security tools, 3% on risk management activities (i.e., NIST 800-37 implementation), 1% on security testing, and 1% on security training. NIST 800-37 requires agencies to apply the Risk Management Framework to Federal information systems using a Security Life Cycle Approach, advancing from the previous periodic Certification and Accreditation (C&A) process into the more continuous Security Authorization Process.

The majority of IT security costs continue to be personnel costs. Making the IT security workforce more productive, more capable, and more collaborative offers one of the most significant opportunities for even more cost-effective IT security spending. This workforce-enabling strategy requires going beyond technical trainings to include process improvement, innovation encouragement, collaboration mechanisms, and accountability structures.

IT Security Personnel

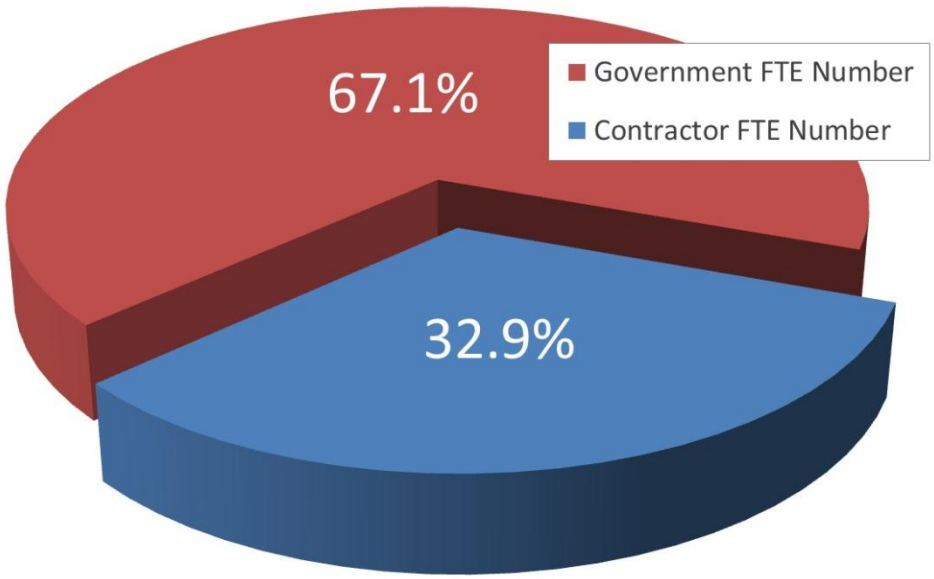
In FY 2012, CFO Act agencies, reported a total of 90,433.09 Full Time Equivalents (FTEs) with major responsibilities in information security. Figure 19 provides a breakout of Total IT Security FTEs by agency.

Figure 19. Total IT Security FTEs Reported by Agencies



Of the total FTEs for the CFO Act agencies, 67% are government FTEs, 33% are contractor FTEs (Figure 20). IT security has consistently been a functional area that depends on talent and technical expertise from industry and commercial sources.

Figure 20. Percentage of Government FTEs Compared to Contractor FTEs



C. 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 Federal Executive Branch. The remaining half is comprised largely of grant-making, advisory, and uniquely chartered organizations. With one exception[35] a "small agency" has less than six thousand employees; most have fewer than five hundred staff. Together these agencies employ about ninety thousand Federal workers and manage billions of taxpayer dollars. Across all Non-CFO Act agencies percentage of FISMA capabilities as reported increased from 55% to 68%.

Summary of Fiscal Year 2012 Non-CFO Act Agencies Reporting Results

In FY 2012, 50 small and micro agencies submitted FISMA reports. The 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 4. Comparison of FISMA Capabilities from FY 2011 to FY 2012 for Non-CFO Act Agencies

Capability Area	FY 2011	FY 2012
Automated Asset Management	79%	87%
Automated Configuration Management	42%	54%
Automated Vulnerability Management	56%	65%
TIC Traffic Consolidation*	35%	62%
TIC 1.0 Capabilities (Includes E2)*	26%	61%
PIV Logical Access (HSPD-12)	1%	3%
Portable Device Encryption	70%	84%
DNSSEC Implementation*	39%	64%
E-Mail Validation Technology*	44%	51%
Remote Access Authentication	71%	91%
Remote Access Encryption*	74%	99%
Controlled Incident Detection*	40%	53%
US-CERT SAR Remediation*	74%	73%
User Training	97%	85%
Users with Security Responsibility Training*	74%	95%
Government-Wide Average	**55%**	**68%**

More details on which Non-CFO Act agencies are included in Table 4 can be found in Appendix 6.

[35] FDIC has approximately 8,000 employees; however, they are following the metrics for micro agencies.

V. Summary of Inspector General's Findings

Each inspector general (IG) was asked to assess his or her department's information security programs in the following eleven 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 96 attributes across these eleven 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.

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 security capital planning, incident response and reporting, and remote access management. The weakest performances occurred in continuous monitoring management, configuration management, POA&M remediation, and identity and access management.

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

Cyber Security Program Area	Program in place		Program not in place	
	FY 2012	%	FY 2012	%
Continuous monitoring	17	71	7	29
Configuration management	18	75	6	25
Identity and access management	20	83	4	17
Incident response and reporting	20	83	4	17
Risk management	18	75	6	25
Security training	22	92	2	8
POA&M	19	79	5	21
Remote access management	20	83	4	17
Contingency planning	18	75	6	25
Contractor systems	18	75	6	25
Security capital planning	19	79	5	21

Table 6 provides the CFO Act agencies' compliance scores. The Department of Defense did not provide sufficient information for scoring. Twelve agencies had programs in place for all eleven areas, although each of these 12 also identified areas for improvement. The other 12 agencies had

at least one area for which it did not have a program. Three agencies - the Department of Housing and Urban Development, the Office of Personnel Management, and the Agency for International Development - reported that they did not have continuous monitoring management programs in place. The numbers of areas with deficiencies were used to compute compliance scores. Eight agencies scored over 90% compliance, 9 scored between 65 and 90% compliance, and the remaining 5 scored less than 65%. The average score was 76%.

Table 6. CFO Act Agencies' Compliance Scores

Agency	FY 2012 (%)
Nuclear Regulatory Commission	99
General Services Administration	99
Department of Homeland Security	99
Social Security Administration	98
Department of Justice	94
National Aeronautics and Space Administration	92
Department of the Interior	92
National Science Foundation	90
Department of Labor	82
Department of Veterans Affairs	81
Department of Education	79
Office of Personnel Management	77
Environmental Protection Agency	77
Department of the Treasury	76
Department of Energy	72
USAID	66
Department of Housing and Urban Development	66
Department of Commerce*	61
Small Business Administration	57
Department of Transportation	53
Department of State	53
Department of Health and Human Services	50
Department of Agriculture	34
Department of Defense**	N/A

* 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.

** DOD did not provide the answers with the detail required for scoring for FY 2012.

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 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 discussed in the sections that follow, the FY 2012 agency FISMA reports indicate improvements in many privacy performance measures despite an increase in the number of systems requiring compliance.

Table 7. Status and Progress of Key Privacy Performance Measures

Performance Measure	FY 2010	FY 2011	FY 2012
Number of systems containing information in identifiable form	3,855	4,282	4,941
Number of systems requiring a Privacy Impact Assessment (PIA)	2,304	2,600	2,778
Number of systems with a PIA	2,135	2,414	2,612
Percentage of systems with a PIA	**93%**	**93%**	**94%**
Number of systems requiring a System of Records Notice (SORN)	2,997	3,366	3,498
Number of systems with a SORN	2,870	3,251	3,339
Percentage of systems with a SORN	**96%**	**97%**	**95%**

Privacy Program Oversight

In FY 2012, 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). The remaining agency reported SAOP participation in two out of the three categories. In addition, all 24 agencies reported having policies in place to ensure that all personnel with access to Federal data are familiar with information privacy requirements, and 23 out of 24 agencies reported having targeted, job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 100% of applicable systems to be covered by publicly posted Privacy Impact Assessments (PIAs). In FY 2012, 94% of applicable systems across the 24 agencies had up-to-date

PIAs covering applicable systems, a 1% increase from 2011. This improvement was achieved in spite of an increase in the number of systems requiring a PIA.

Written Policies for Privacy Impact Assessments and Web Privacy Practices

In FY 2012, all 24 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; and
- Making appropriate updates and ensuring continued compliance with stated web privacy policies.

In addition, 23 out of 24 agencies reported having written policies in place for these topics:

- 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.

Finally, 22 out of 24 agencies reported having written policies in place for this topic:

- 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 system of records notice (SORN). In FY 2012, 95% of information systems across Government with records subject to the Privacy Act have published corresponding SORNs. This reflects a 2% decrease in compliance from 2011, which occurred while the number of applicable systems increased.

Agency Use of Web Management and Customization Technologies

In FY 2012, 22 out of 24 agencies reported use of web management and customization technologies. All 22 of those agencies reported having procedures for annual review, continued justification and approval for, and public notice of their use of web management and customization technologies.

VII. Appendices

Appendix 1: NIST Performance in 2012

The E-Government Act, Public Law 107-347, passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) of 2002, included duties and responsibilities for the National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division (CSD). In 2012, CSD addressed its assignments through the following activities:

- Issued one final and two draft Federal Information Processing Standards (FIPS) that specify hash algorithms used to generate message digests, algorithms used to generate digital signatures, and technical requirements for a common identification standard for Federal employees and contractors;
- Issued 28 draft and final NIST Special Publications (SPs) that provide management, operational, and technical security guidelines in areas such as Basic Input Output System (BIOS) management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, and risk assessments. In addition, 12 draft and final NIST Interagency Reports were issued on a variety of topics including supply chain risk management, personal identity verification, access control, security automation and continuous monitoring, and the Smart Grid Advanced Metering Infrastructure;
- Produced guidelines concerning the handling of information security incidents to help agencies analyze incident-related data and determine the appropriate response to each incident;
- Continued the successful collaboration with the Office of the Director of National Intelligence, the Committee on National Security Systems, and the Department of Defense to establish a common foundation for information security across the Federal Government, including a structured, yet flexible approach for managing information security risk across an organization. In 2012, this collaboration produced foundational guidelines for conducting risk assessments, and updated guidelines for selecting and specifying security controls for Federal information systems and organizations;
- Provided assistance to agencies and the private sector: conducted ongoing, substantial reimbursable and non-reimbursable assistance to the government and private sector, including many outreach efforts through the Federal Information Systems Security Educators' Association (FISSEA), the Federal Computer Security Program Managers' Forum, and the Small Business Information Security Corner;
- Reviewed security policies and technologies from the private sector and national security systems for potential Federal agency use: hosted a repository of Federal agency security practices, public/private security practices, and security configuration checklists for IT products. Continued to lead, in conjunction with the Government of Canada's Communications Security Establishment, the Cryptographic Module Validation Program (CMVP). The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate security testing of IT products usable by the Federal Government;

- Solicited recommendations of the Information Security and Privacy Advisory Board (ISPAB) on draft standards and guidelines and on information security and privacy issues regularly at board meetings scheduled three times per year;
- Conducted workshops, awareness briefings and outreach to CSD customers to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open and transparent manner. CSD also held workshops on diverse information security and technology topics including security automation, identity management, information and communications technologies supply chain risk management, information security awareness and training, cybersecurity of cyber physical systems, technical aspects of botnets, health information security, and mobile computing; and
- Produced an annual report as a NIST Interagency Report (NISTIR). The 2003-2011 Annual Reports are available on the Computer Security Resource Center (CSRC) at http://csrc.nist.gov.

Appendix 2: Security Incidents by CFO Act Agency

The following agency specific figures provide incident frequencies.

Figure 21. Security Incidents - Department of Agriculture

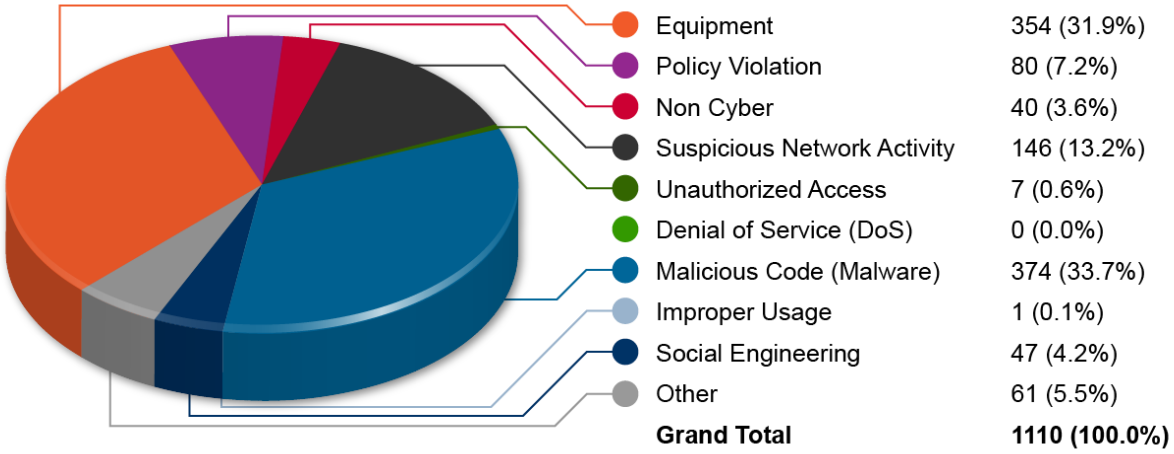


Figure 22. Security Incidents - Department of Commerce

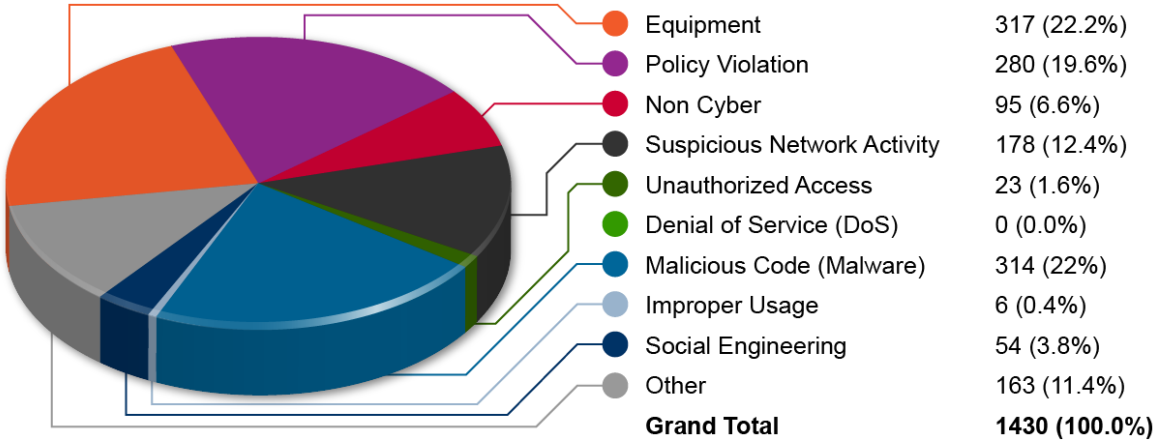
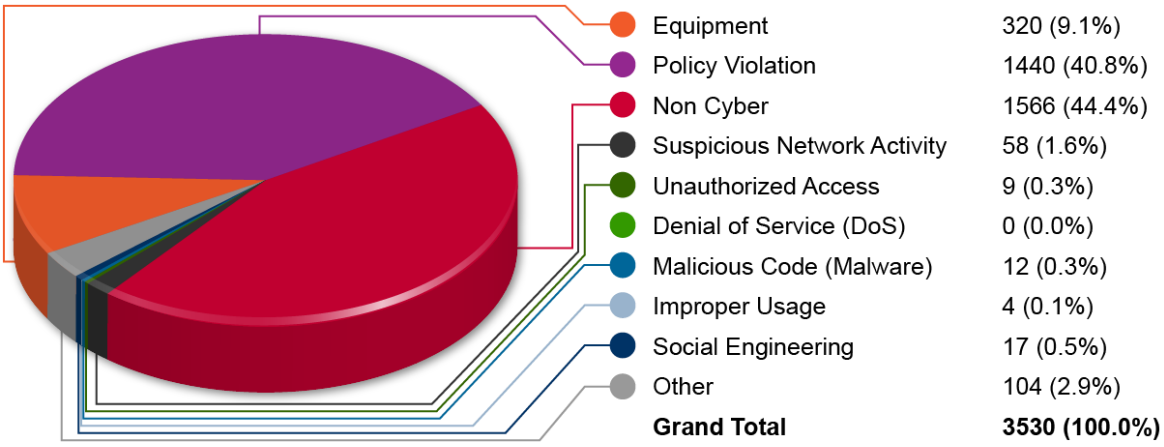
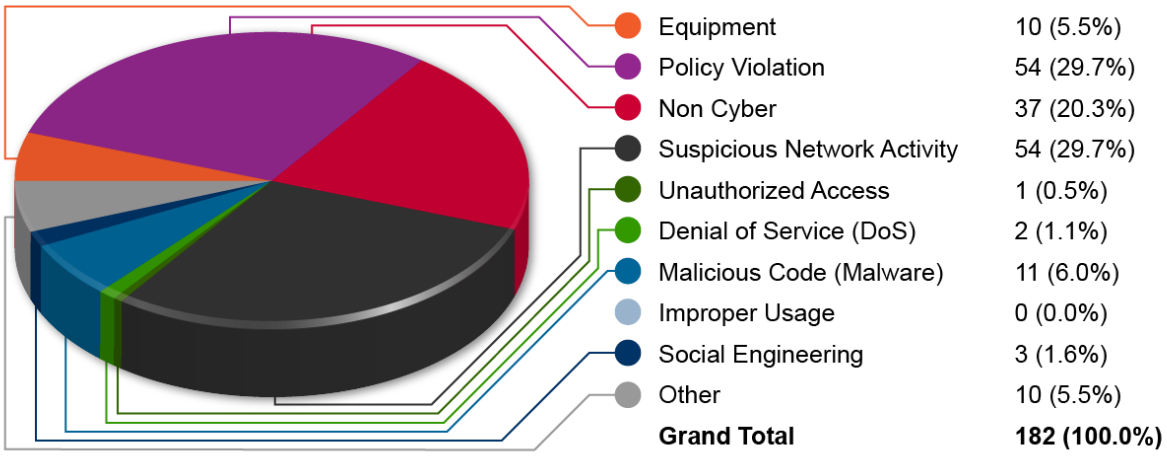


Figure 23. Security Incidents - Department of Defense



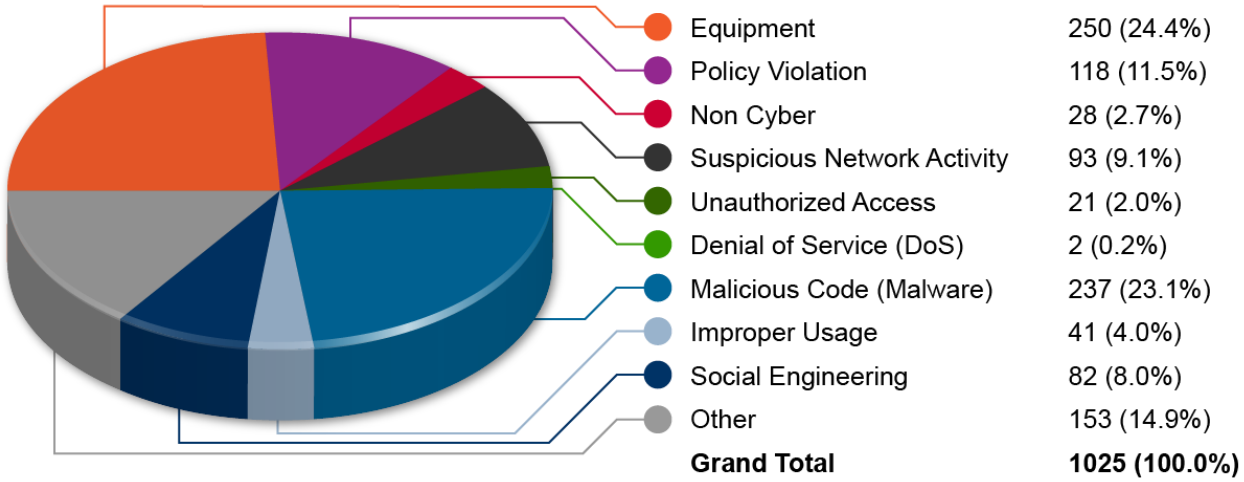
Equipment	320 (9.1%)
Policy Violation	1440 (40.8%)
Non Cyber	1566 (44.4%)
Suspicious Network Activity	58 (1.6%)
Unauthorized Access	9 (0.3%)
Denial of Service (DoS)	0 (0.0%)
Malicious Code (Malware)	12 (0.3%)
Improper Usage	4 (0.1%)
Social Engineering	17 (0.5%)
Other	104 (2.9%)
Grand Total	**3530 (100.0%)**

Figure 24. Security Incidents - Department of Education



Equipment	10 (5.5%)
Policy Violation	54 (29.7%)
Non Cyber	37 (20.3%)
Suspicious Network Activity	54 (29.7%)
Unauthorized Access	1 (0.5%)
Denial of Service (DoS)	2 (1.1%)
Malicious Code (Malware)	11 (6.0%)
Improper Usage	0 (0.0%)
Social Engineering	3 (1.6%)
Other	10 (5.5%)
Grand Total	**182 (100.0%)**

Figure 25. Security Incidents - Department of Energy



Equipment	250 (24.4%)
Policy Violation	118 (11.5%)
Non Cyber	28 (2.7%)
Suspicious Network Activity	93 (9.1%)
Unauthorized Access	21 (2.0%)
Denial of Service (DoS)	2 (0.2%)
Malicious Code (Malware)	237 (23.1%)
Improper Usage	41 (4.0%)
Social Engineering	82 (8.0%)
Other	153 (14.9%)
Grand Total	**1025 (100.0%)**

Figure 26. Security Incidents - Department of Health and Human Services

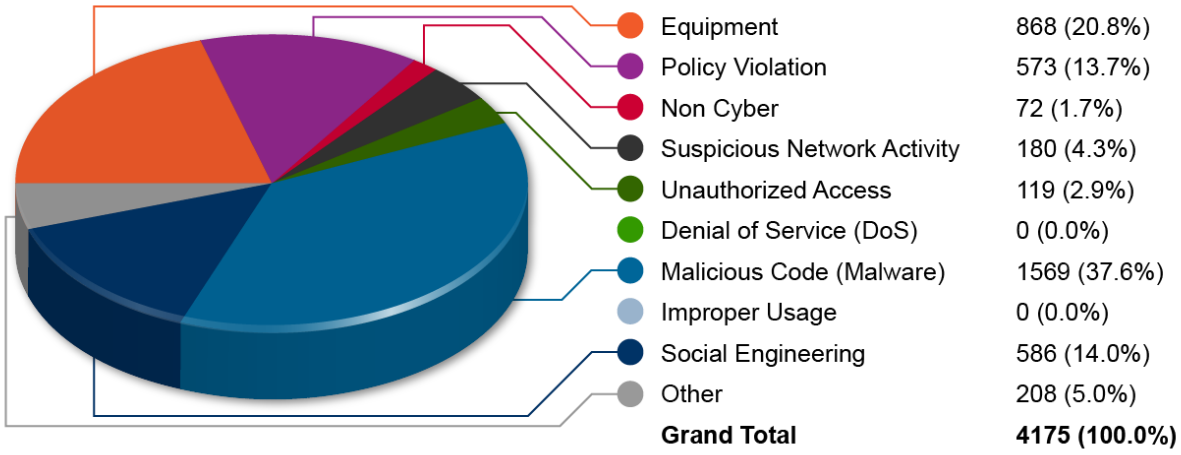


Figure 27. Security Incidents - Department of Homeland Security

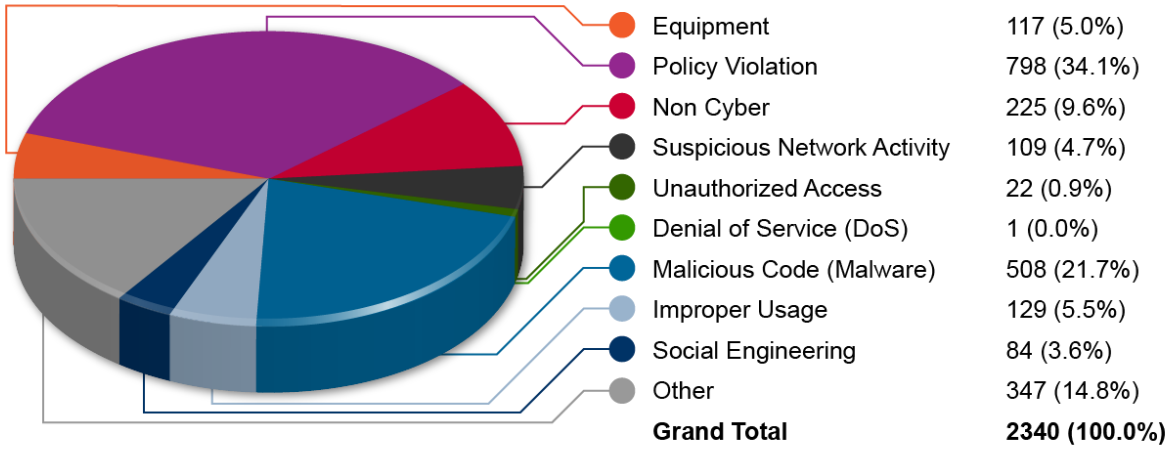


Figure 28. Security Incidents - Department of Housing and Urban Development

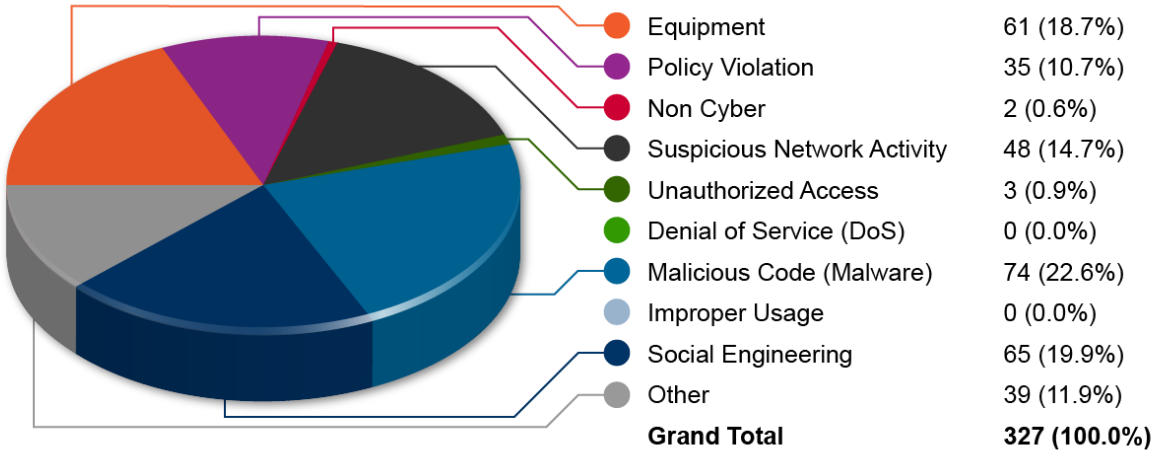


Figure 29. Security Incidents - Department of the Interior

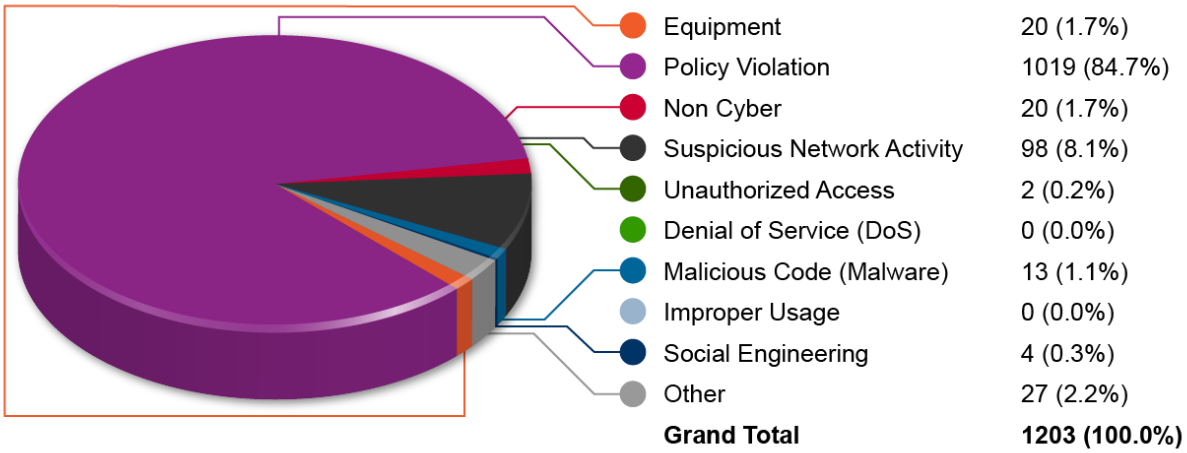


Figure 30. Security Incidents - Department of Justice

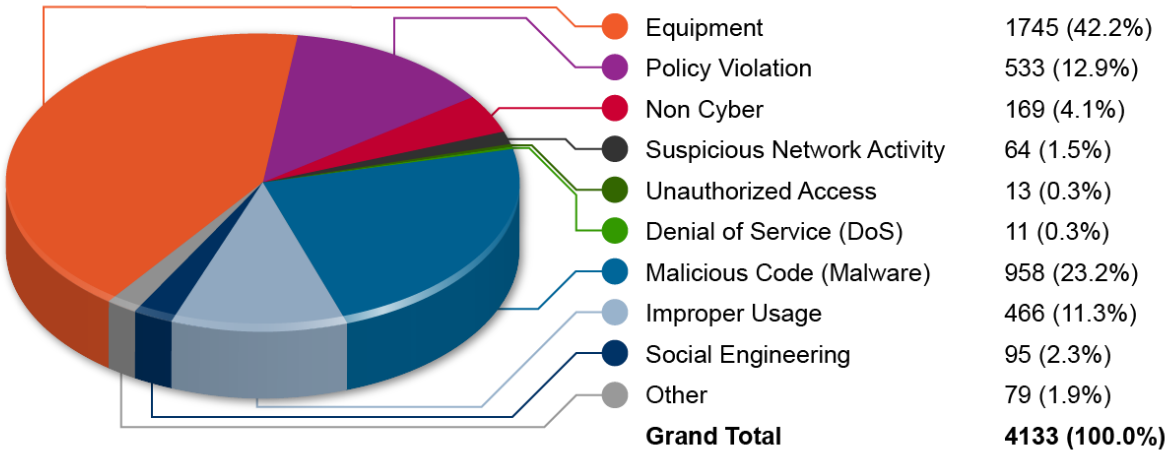


Figure 31. Security Incidents - Department of Labor

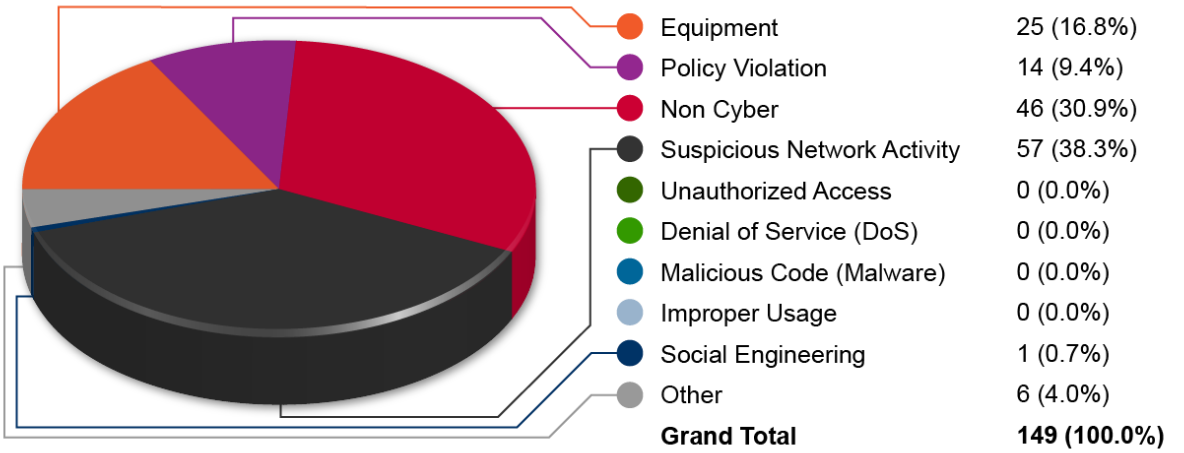
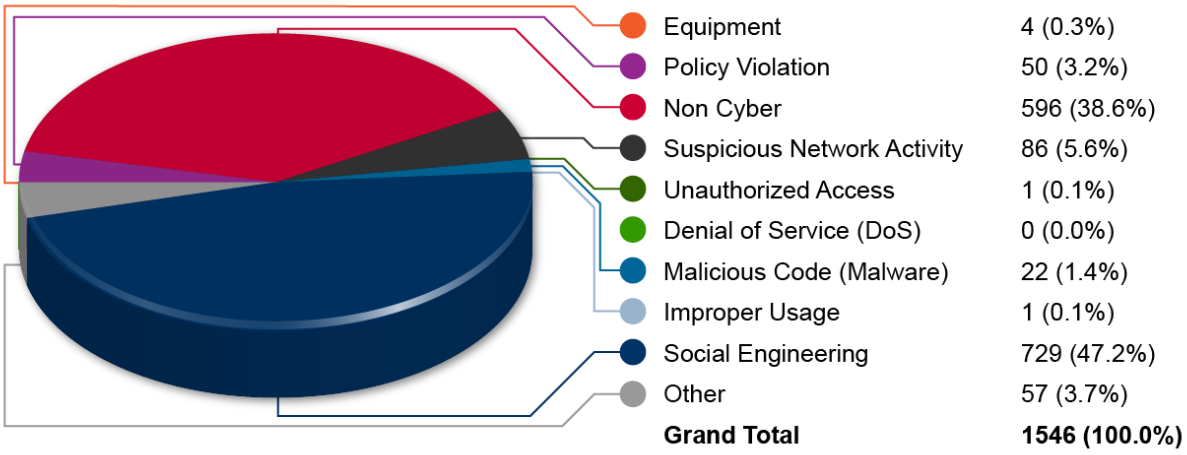
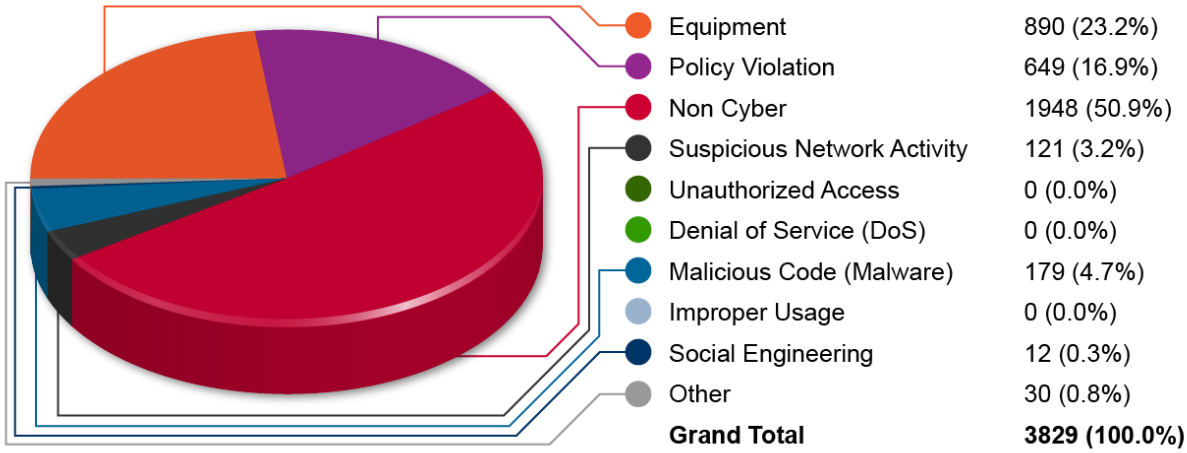


Figure 32. Security Incidents - Department of State



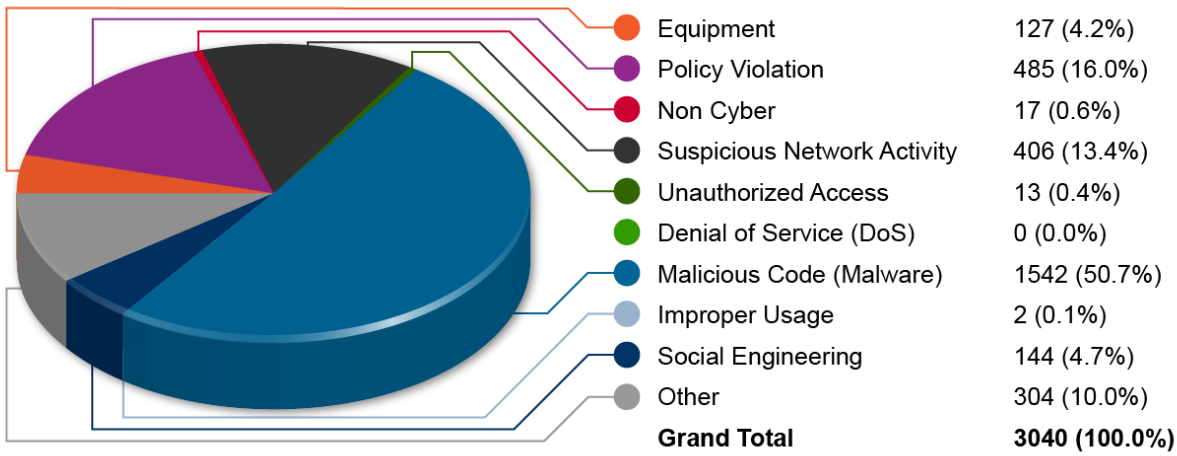
Equipment	4 (0.3%)
Policy Violation	50 (3.2%)
Non Cyber	596 (38.6%)
Suspicious Network Activity	86 (5.6%)
Unauthorized Access	1 (0.1%)
Denial of Service (DoS)	0 (0.0%)
Malicious Code (Malware)	22 (1.4%)
Improper Usage	1 (0.1%)
Social Engineering	729 (47.2%)
Other	57 (3.7%)
Grand Total	**1546 (100.0%)**

Figure 33. Security Incidents - Department of the Treasury



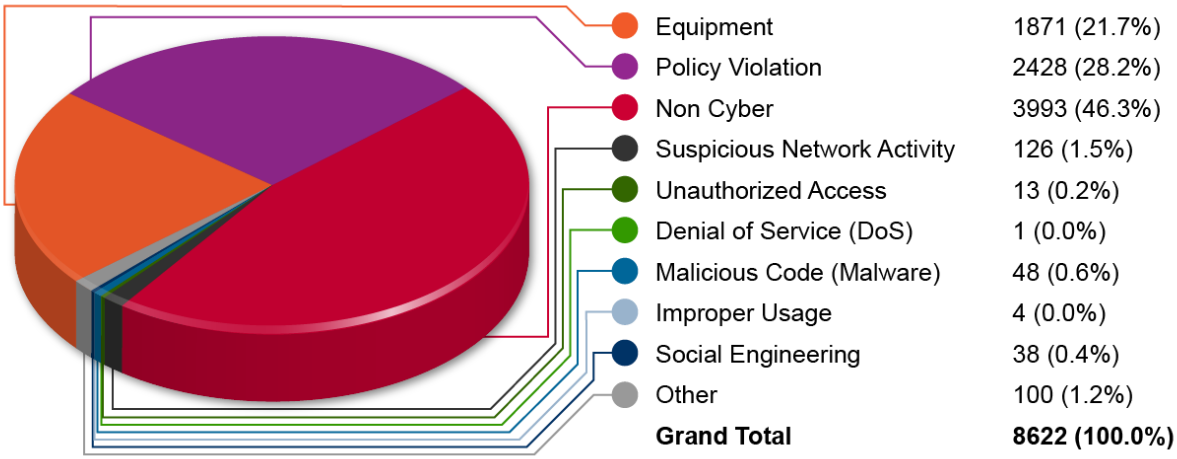
Equipment	890 (23.2%)
Policy Violation	649 (16.9%)
Non Cyber	1948 (50.9%)
Suspicious Network Activity	121 (3.2%)
Unauthorized Access	0 (0.0%)
Denial of Service (DoS)	0 (0.0%)
Malicious Code (Malware)	179 (4.7%)
Improper Usage	0 (0.0%)
Social Engineering	12 (0.3%)
Other	30 (0.8%)
Grand Total	**3829 (100.0%)**

Figure 34. Security Incidents - Department of Transportation



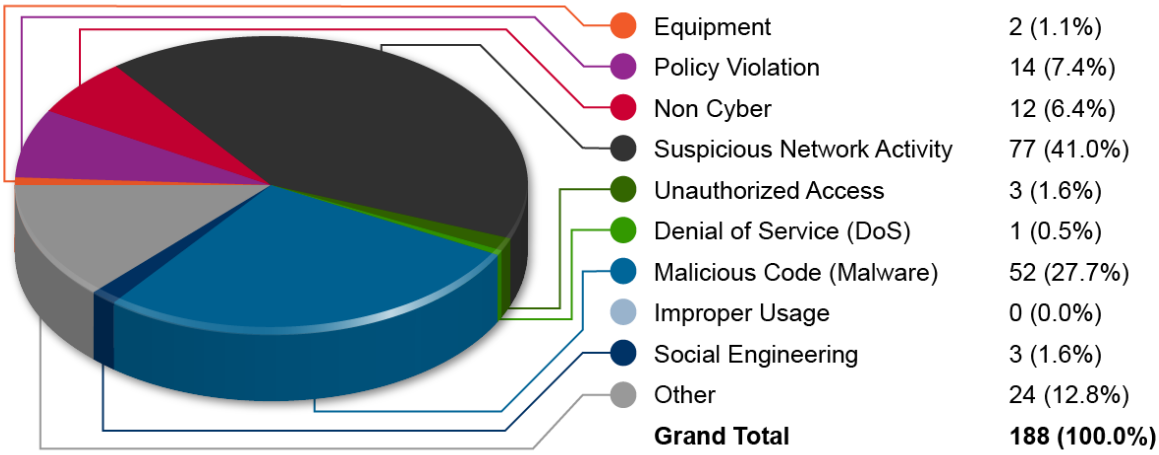
Equipment	127 (4.2%)
Policy Violation	485 (16.0%)
Non Cyber	17 (0.6%)
Suspicious Network Activity	406 (13.4%)
Unauthorized Access	13 (0.4%)
Denial of Service (DoS)	0 (0.0%)
Malicious Code (Malware)	1542 (50.7%)
Improper Usage	2 (0.1%)
Social Engineering	144 (4.7%)
Other	304 (10.0%)
Grand Total	**3040 (100.0%)**

Figure 35. Security Incidents - Department of Veteran Affairs



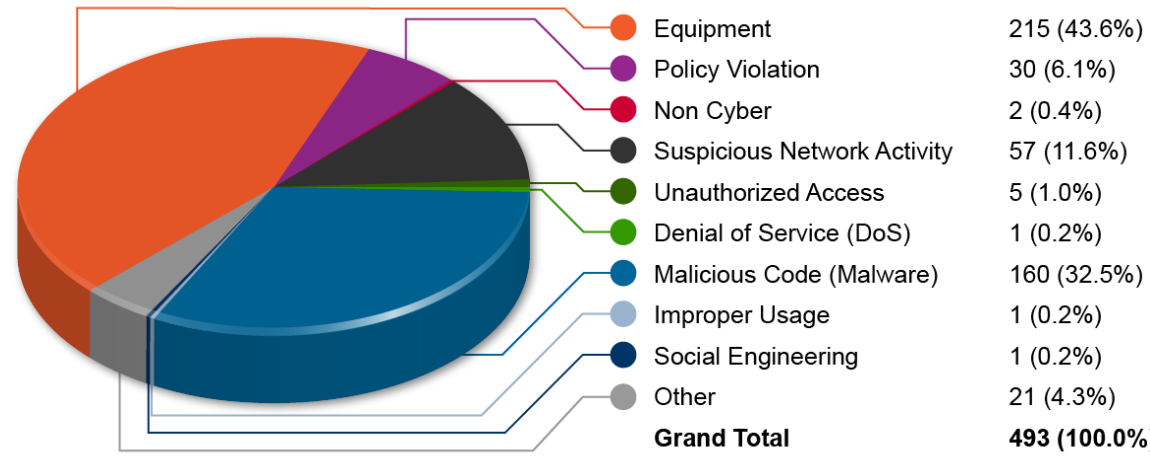
Equipment	1871 (21.7%)
Policy Violation	2428 (28.2%)
Non Cyber	3993 (46.3%)
Suspicious Network Activity	126 (1.5%)
Unauthorized Access	13 (0.2%)
Denial of Service (DoS)	1 (0.0%)
Malicious Code (Malware)	48 (0.6%)
Improper Usage	4 (0.0%)
Social Engineering	38 (0.4%)
Other	100 (1.2%)
Grand Total	**8622 (100.0%)**

Figure 36. Security Incidents - Environmental Protection Agency



Equipment	2 (1.1%)
Policy Violation	14 (7.4%)
Non Cyber	12 (6.4%)
Suspicious Network Activity	77 (41.0%)
Unauthorized Access	3 (1.6%)
Denial of Service (DoS)	1 (0.5%)
Malicious Code (Malware)	52 (27.7%)
Improper Usage	0 (0.0%)
Social Engineering	3 (1.6%)
Other	24 (12.8%)
Grand Total	**188 (100.0%)**

Figure 37. Security Incidents - General Services Administration



Equipment	215 (43.6%)
Policy Violation	30 (6.1%)
Non Cyber	2 (0.4%)
Suspicious Network Activity	57 (11.6%)
Unauthorized Access	5 (1.0%)
Denial of Service (DoS)	1 (0.2%)
Malicious Code (Malware)	160 (32.5%)
Improper Usage	1 (0.2%)
Social Engineering	1 (0.2%)
Other	21 (4.3%)
Grand Total	**493 (100.0%)**

Figure 38. Security Incidents - National Aeronautics and Space Administration

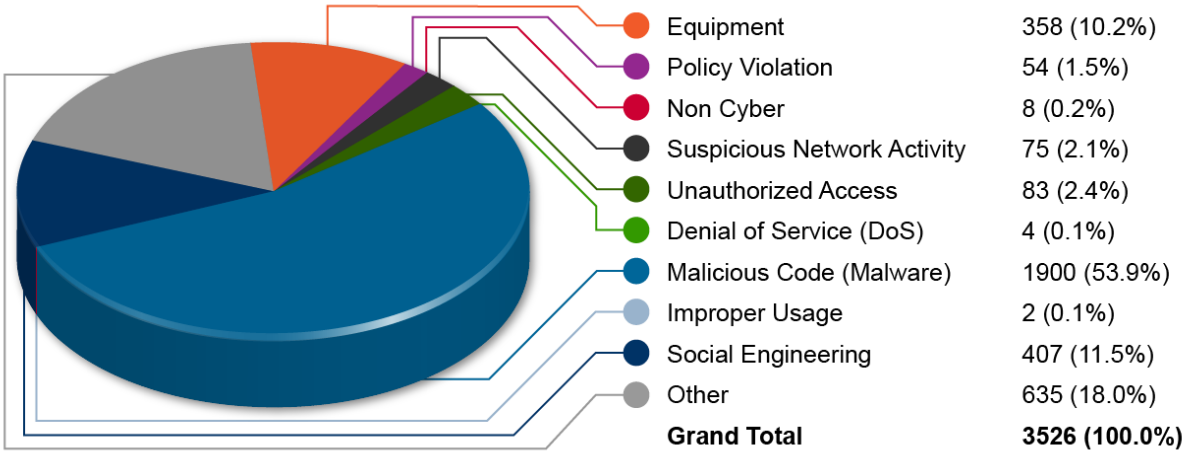


Figure 39. Security Incidents - National Science Foundation

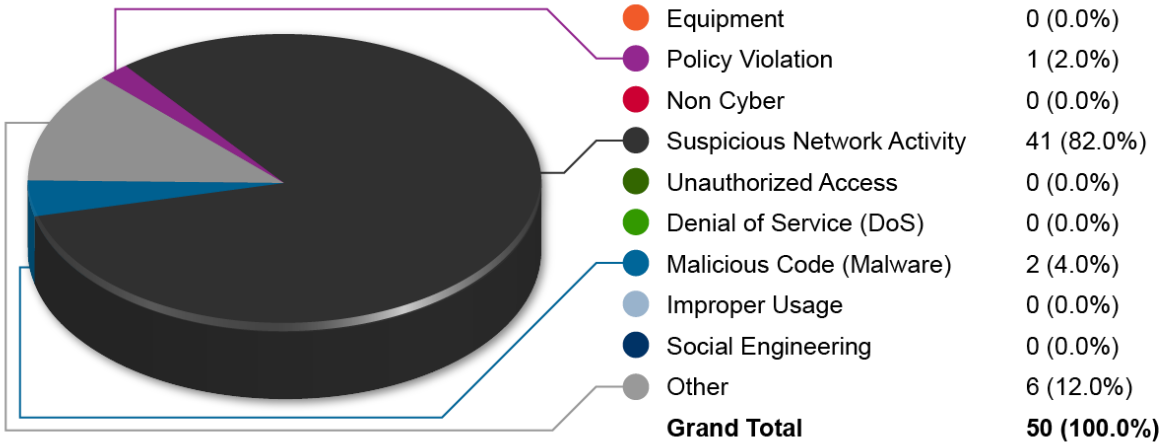


Figure 40. Security Incidents - Nuclear Regulatory Commission

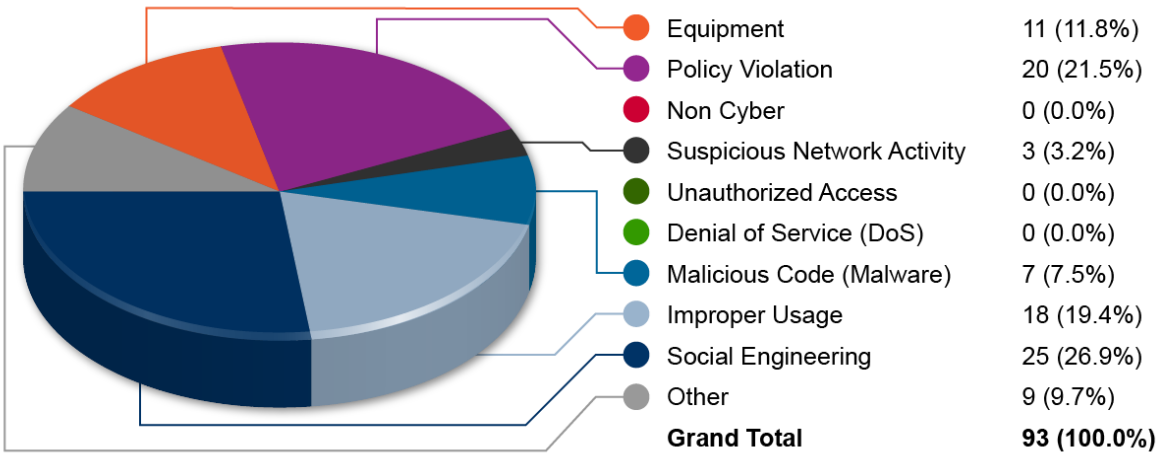


Figure 41. Security Incidents - Office of Personnel Management

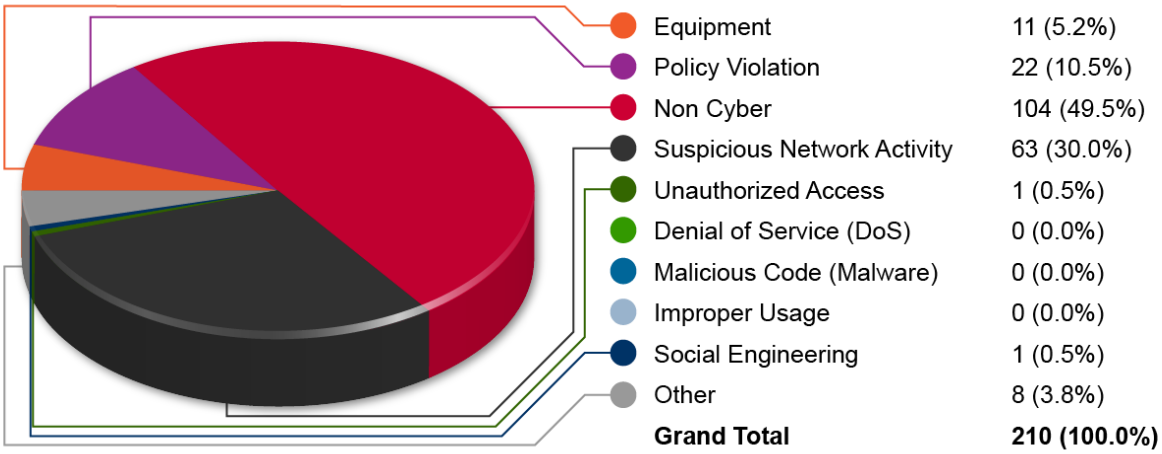


Figure 42. Security Incidents - Small Business Administration

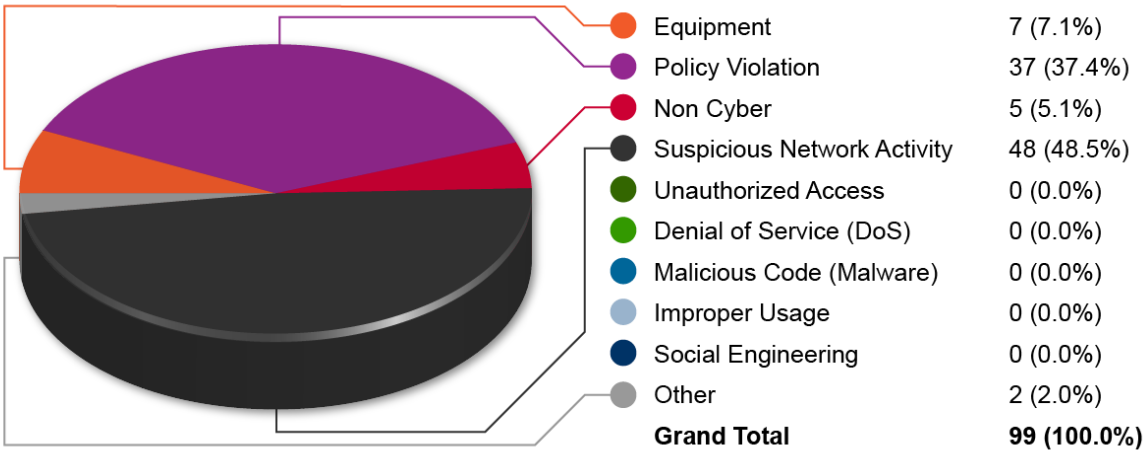


Figure 43. Security Incidents - Social Security Administration

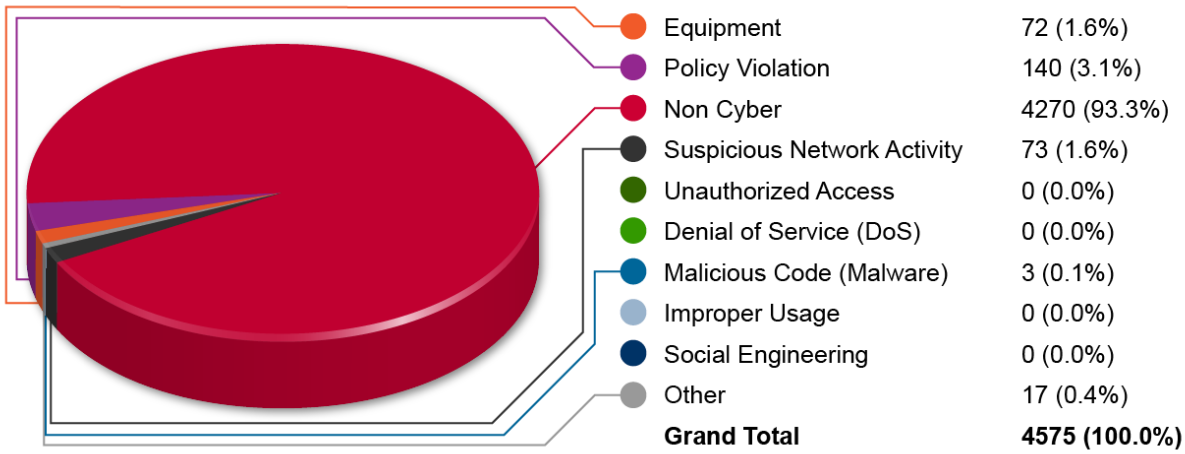
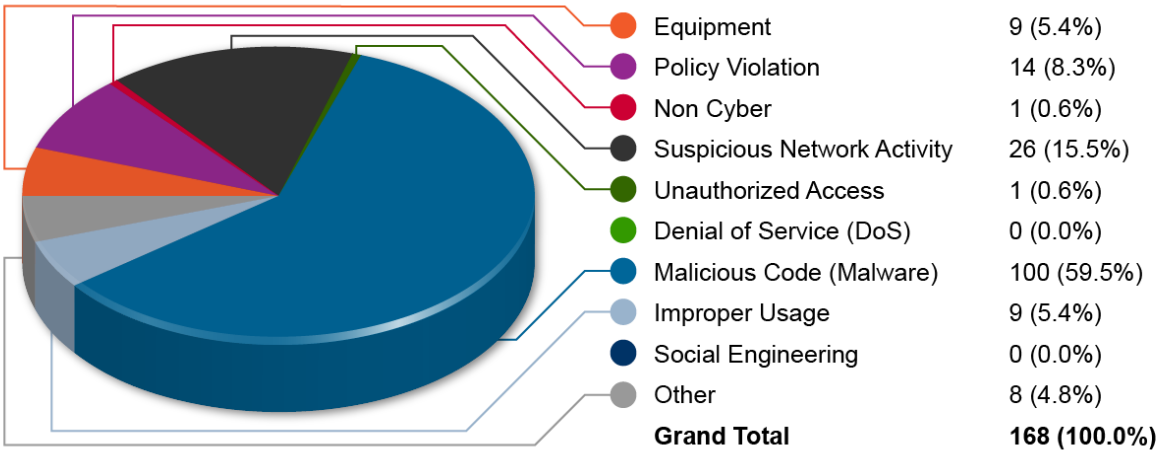


Figure 44. Security Incidents - US Agency for International Development



Appendix 3: IT Security Spending Reported by CFO Act Agencies

The following data for CFO Act agencies is from the OMB Exhibit 53B Agency IT Security Portfolio section.

	Personnel				Other FISMA Costs				
Agency	*Government FTEs**	Average Cost per Gov't FTE	*Contractor FTEs**	Average Cost per Contr. FTE	NIST SP 800-37 Implementation**	Tools Cost	Testing Cost	Training Cost	Total Costs
DOD	*54,934.00*	$141,732	*25,532.44*	$150,000	$54,819,000	$239,364,000	$36,060,000	$110,746,000	**$12,056,760,688**
DHS	*395.44*	$118,565	*635.52*	$178,254	$147,744,860	$296,874,070	$7,352,880	$3,382,900	**$615,523,830**
Treasury	*1,745.08*	$149,902	*663.10*	$148,065	$16,818,180	$17,775,590	$2,893,670	$6,724,660	**$403,984,501**
Justice	*311.00*	$138,315	*434.49*	$217,854	$35,962,426	$21,350,840	$17,874,940	$3,265,181	**$216,124,736**
Energy	*58.75*	$124,594	*634.32*	$205,553	$28,360,423	$34,659,841	$10,209,487	$3,724,727	**$214,660,754**
HHS	*335.20*	$136,415	*376.85*	$208,347	$11,199,237	$24,516,960	$30,271,997	$1,266,383	**$191,496,663**
SSA	*1,145.00*	$128,997	*22.50*	$178,500	$4,540,900	$9,375,400	$967,500	$552,500	**$167,154,115**
Commerce	*323.37*	$162,257	*174.77*	$198,883	$24,358,610	$27,735,651	$12,710,420	$2,974,421	**$155,006,930**
DOT	*241.69*	$178,031	*90.86*	$219,799	$22,755,048	$27,755,678	$2,291,969	$271,238	**$116,073,256**
VA	*530.00*	$106,000	*222.00*	$185,000	$4,182,000	$6,514,000	$2,679,000	$1,313,000	**$111,938,000**
NASA	*92.75*	$137,414	*283.70*	$156,836	$2,851,000	$4,181,000	$981,000	$501,000	**$65,753,489**
USDA	*18.00*	$118,254	*157.45*	$134,715	$14,100,400	$13,543,039	$10,415,000	$529,556	**$61,927,444**
Interior	*131.67*	$101,893	*166.25*	$116,558	$6,330,427	$7,430,050	$3,662,204	$193,432	**$50,410,132**
Labor	*83.31*	$128,564	*60.08*	$211,125	$2,686,965	$3,382,452	$4,643,636	$319,792	**$34,427,902**
State	*86.00*	$135,000	*1.75*	$175,000	$8,196,169	$3,908,953	$3,788,780	$192,000	**$28,002,152**
EPA	*30.00*	$124,415	*61.50*	$138,135	$11,117,727	$2,763,300	$339,547	$75,206	**$26,523,533**
ED	*37.00*	$105,000	*48.00*	$142,000	$4,523,000	$3,222,000	$1,322,000	$217,000	**$19,985,000**
GSA	*45.00*	$143,140	*39.00*	$172,640	$3,553,110	$2,436,440	$575,430	$110,000	**$19,849,240**
HUD	*117.00*	$100,000	*21.00*	$50,000	$1,250,000	$245,000	$400,000	$60,000	**$14,705,000**
NSF	*7.00*	$293,877	*30.00*	$286,738	$1,171,534	$1,071,931	$744,129	$34,375	**$13,681,236**
OPM	*30.09*	$129,880	*17.61*	$212,960	$3,472,840	$1,458,180	$412,220	$112,460	**$13,114,015**
NRC	*17.25*	$151,000	*25.00*	$200,000	$1,692,000	$2,258,000	$478,000	$180,000	**$12,212,750**
SBA	*8.80*	$125,000	*11.50*	$224,544	$634,923	$266,390	$21,899	$19,754	**$4,625,222**
USAID	*0.00*	$198,693	*0.00*	$207,640	$241,877	$1,709,306	$123,717	$12,000	**$2,086,900**
TOTAL	***60,723.40***	-	***29,709.69***	-	**$412,562,656**	**$753,798,071**	**$151,219,425**	**$136,777,585**	**$14,616,027,487**

*Note: FTEs are normalized so that personnel costs included in other categories are not included in this column.

**Note: NIST Special Publication 800-37 is the Risk Management Framework Implementation.

Appendix 4: Inspectors General's Response

Each inspector general (IG) was asked to assess his or her department's information security programs in the following eleven 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 96 attributes across these eleven 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.

Table 8 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 security capital planning, incident response and reporting, and remote access management. The weakest performances occurred in continuous monitoring management, configuration management, POA&M remediation, and identity and access management.

Table 8. Results for CFO Act Agencies by Cyber Security Area

	Program in place		Program not in place	
Cyber Security Program Area	**FY 2012**	**%**	**FY 2012**	**%**
Continuous monitoring	17	71	7	29
Configuration management	18	75	6	25
Identity and access management	20	83	4	17
Incident response and reporting	20	83	4	17
Risk management	18	75	6	25
Security training	22	92	2	8
POA&M	19	79	5	21
Remote access management	20	83	4	17
Contingency planning	18	75	6	25
Contractor systems	18	75	6	25
Security capital planning	19	79	5	21

Table 9 provides the CFO Act agencies' compliance scores. The Department of Defense did not provide sufficient information for scoring. Twelve large agencies had programs in place for all eleven areas, although each of these 12 also identified areas for improvement. The other 12 agencies had at least one area for which it did not have a program. Three agencies - the Department of Housing and Urban Development, the Office of Personnel Management, and the Agency for International Development - reported that they did not have continuous monitoring management programs in place. The numbers of areas with deficiencies were used to

compute compliance scores. Eight agencies scored over 90% compliance, 9 scored between 65 and 90% compliance, and the remaining 5 scored less than 65%. The average score was 76%.

Table 9. CFO Act Agencies' Compliance Scores

Agency	FY 2012 (%)
Nuclear Regulatory Commission	99
General Services Administration	99
Department of Homeland Security	99
Social Security Administration	98
Department of Justice	94
National Aeronautics and Space Administration	92
Department of the Interior	92
National Science Foundation	90
Department of Labor	82
Department of Veterans Affairs	81
Department of Education	79
Office of Personnel Management	77
Environmental Protection Agency	77
Department of the Treasury	76
Department of Energy	72
USAID	66
Department of Housing and Urban Development	66
Department of Commerce*	61
Small Business Administration	57
Department of Transportation	53
Department of State	53
Department of Health and Human Services	50
Department of Agriculture	34
Department of Defense**	N/A

* 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.
** DOD did not provide the answers with the detail required for scoring for FY2012.

The Eleven Cyber Security Areas

Continuous Monitoring

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. Continuous monitoring 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:

- Ongoing assessments of security controls (system-specific, hybrid, and common) had not been performed based on the approved continuous monitoring plans (9 departments);
- The department lacked documented strategies and plans for continuous monitoring (7 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, 18 of 24 agencies had configuration management programs in place. However, only one IG 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:

- Patch management process was not fully developed (15 departments);
- Configuration-related vulnerabilities, including scan findings, had not been remediated in a timely manner (14 departments);
- Software assessment capabilities were not fully implemented (14 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. Homeland Security Directive 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, Government wide account and identity management system.

Identity and access management was identified as another area in need of improvement. Twenty of the 24 IGs reported that their departments had identity and access management programs in place. The most common control weaknesses were:

- The department did not ensure that accounts were terminated or deactivated once access was no longer required (12 departments);
- The department did not ensure that the users are granted access based on needs and separation of duties principles (11 departments);
- The department's mult-factor authentication system was not linked to its PIV program where appropriate (11 departments).

Incident Response and Reporting

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

Incident response and reporting programs were largely compliant. Twenty IGs reported that their departments had incident response and reporting programs in place. However, 11 of 23 IGs identified at least one missing component. The following deficiencies were most common:

- Reports to US-CERT were not made within established timeframes (4 departments);
- The department did not respond to and resolve incidents in a timely manner (4 departments);
- The department was not capable of correlating incidents (4 departments);
- There was insufficient incident monitoring and detection coverage (4 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.

Eighteen IGs reported that their departments had risk management programs in place. However, only 2 of the 18 reported complete programs, while 16 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 (10 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 (9 departments);
- 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 (9 departments).

Security Training

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

Security training was the highest scoring metric. Twenty-two IGs reported that their departments had compliant programs. Fifteen of these 22 reported that their departments' programs included all of the required elements. Among the eight 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 (4 departments);
- Identification and tracking of the status of specialized training was not completed for all personnel with significant information security responsibilities that required specialized training (4 departments).

POA&M Remediation

When it identifies weaknesses in information security systems as the result of controls testing, audits, incidents, continuous monitoring, or other means, a department 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.

Nineteen IGs reported that their departments had POA&Ms in place. Of these 19, 8 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 had not established and adhered to milestone remediation dates (11 departments);
- The department did not ensure remediation plans were effective for correcting weaknesses (10 departments);
- The department did not track, prioritize and remediate weaknesses (8 departments);
- The department did not ensure that resources were provided for correcting weaknesses (8 departments);
- Costs associated with weakness remediation were not identified (8 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, not required for local access.

Twenty IGs reported that their departments had remote access management programs in place, and ten of these had all required attributes. The remaining IGs reported at least 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 (5 departments);
- Multi-factor authentication was not required for remote access (5 departments).

Contingency Planning

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

Eighteen IGs reported that their departments had contingency planning programs in place. However, only 5 reported that their departments' contingency planning programs were fully compliant with standards. The following issues were prevalent among the 18 departments that needed improvements:

- The department had not performed an overall Business Impact Analysis (11 departments);
- Alternate processing sites were subject to the same risks as primary sites (9 departments);
- Neither regular ongoing testing nor exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans was performed (8 departments);
- The department did not have an alternate processing site (8 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.

Eighteen IGs reported that their departments had programs in place to manage contractor systems, but only nine reported that their departments' programs included all required attributes. Fourteen 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 (9 departments);
- 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 (9 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.

Nineteen IGs reported that their departments had security capital planning programs in place, and 15 of these included all required attributes. Eight 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 (5 departments).

The department's CPIC information security policies and procedures were not fully developed (4 departments).

Appendix 5: List of Chief Financial Officer (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 the Treasury	Treasury
Department of Transportation	DOT
Department of Veterans Affairs	VA
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
United States Agency for International Development	USAID

Appendix 6: List of Non-Chief Financial Officer (CFO) Act Agencies Reporting to CyberScope

Non-CFO Act Agency	Acronym
Armed Forces Retirement Home	AFRH
Broadcasting Board of Governors	BBG
Chemical Safety Board †	CSB
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 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
National Archives and Records Administration	NARA
National Capital Planning Commission †	NCPC
National Council on Disability †	NCD
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
Office of Government Ethics †	OGE

Non-CFO Act Agency	Acronym
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
Securities and Exchange Commission *	SEC
Smithsonian Institution	SI
Tennessee Valley Authority	TVA

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

†Micro Agency