Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

March 7, 2012

Table of Contents

List of Figures

List of Tables

I. Introduction: Current State of Federal Information Security

The Federal Government serves the public by providing thousands of essential services, 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 this IT infrastructure – 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 governmental IT 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 FISMA. This *Fiscal Year 2011 FISMA Report to Congress* provides the annual status of Federal-wide and Agency-specific information security initiatives with respect to Federal compliance with FISMA requirements.

Among accomplishments, in Fiscal Year (FY) 2011 the Federal Government:

- Established Administration priorities with executive-level oversight to ensure progress on the capability areas of continuous monitoring, Trusted Internet Connection (TIC) compliance and traffic consolidation, and HSPD-12 implementation for logical access.
- Updated the FISMA metrics to increase granularity for greater visibility and insight into agency cybersecurity capabilities and effectiveness.
- Conducted the first CyberStat reviews with agencies to examine the metrics reported through CyberScope and develop in-depth remediation plans to quickly address and correct any weaknesses identified in their cybersecurity program.
- Developed agency action plans to drive increasingly mature security performance metrics.
- Continued the shift from three-year security reauthorization to continuous monitoring of information systems.
- Concentrated efforts on Domain Name System Security (DNSSEC) and Email Security through the creation of a government-wide technical Tiger Team and the release of technical reference architectures for DNS and Email Security Gateway.
- Established the Chief Information Security Officer (CISO) Advisory Council to enhance collaboration and information sharing across the government.

---

[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

- Released four Cybersecurity Workforce Development Matrices and the accompanying Cybersecurity Workforce Development Matrix Resource Guide.[3]

Another significant accomplishment in FY 2011 was a focus on detailed, quantitative, outcome-focused security metrics, exported from agency tools and submitted to CyberScope, the Federal repository for collecting FISMA data. Many metrics were carried over from FY 2010, which established a baseline and provided the first FY 2010, FY 2011 opportunity to measure progress in the cybersecurity posture of both individual agencies and Federal government as a whole.

Additionally, in May 2011, the Administration transmitted a cybersecurity legislative proposal to Congress. The Administration proposal seeks to clarify and codify current Department of Homeland Security (DHS) responsibilities in areas of protecting Federal civilian agencies and assisting in the protection of critical information infrastructure across of range of activities. The proposal includes a specific authorization for DHS to conduct risk assessments – including threat, vulnerability and impact assessments as well as penetration testing for Federal systems and requesting critical infrastructure entities. The proposed language gives statutory clarity to current reforms and OMB delegations of operational responsibility to DHS. The proposal builds upon DHS efforts currently underway for Federal systems, and includes provisions related to voluntary information sharing and addressing potential liability concerns.

[3] CIO Council Releases Cybersecurity Workforce Development Matrices, released December 5th 2011, available at: http://www.cio.gov/pages-nonnews.cfm/page/CIO-Council-Releases-Cybersecurity-Workforce-Development-Matrices

II. FY 2011 Progress

This past year reflected improvements in FISMA efforts, through the automated submission and collection of quantitative FISMA data, the establishment of a year-to-year baseline through the continuation of outcome-based FY 2010 FISMA metrics, and the narrowing of FISMA efforts to allocate limited resources to the most pressing Federal cybersecurity challenges. These improvements have greatly informed our understanding of current cybersecurity posture and have helped to drive accountability towards improving the collective effectiveness of our cybersecurity capabilities.

In 2010, OMB designated DHS as the lead agency to establish baseline Cybersecurity metrics for the Federal Government[4]. With this charge, DHS Cybersecurity experts continued to improve the metrics and collected the associated data which have provided the Administration greater insights into strengths and weaknesses of the Agencies' security posture. In FY 2011, agencies reported that security capability areas remained the same or improved (with the exception of Controlled Incident Detection[5]). While cybersecurity metrics are applicable to all within the Federal Executive Branch, this report summarizes data collected from the Chief Financial Officer (CFO) Act agencies.

Table 1. Comparison of FISMA Capabilities from FY 2010 to FY 2011

Capability Area	FY 10	FY 11
Automated Asset Management	66%	80%
Automated Configuration Management	50%	78%
Automated Vulnerability Management	51%	77%
TIC Traffic Consolidation	48%	65%
TIC 1.0 Capabilities (Includes E2)	60%	72%
PIV Logical Access (HSPD-12)	55%	66%
Portable Device Encryption	54%	83%
DNSSEC Implementation	35%	65%
E-Mail Validation Technology	46%	58%
Remote Access Authentication	52%	52%
Remote Access Encryption	72%	83%
Controlled Incident Detection	70%	49%
US CERT SAR Remediation	90%	97%
User Training	92%	99%
Privileged User Training	88%	92%
Government-Wide Average	62%	74%

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

[5] According to DHS, a number of agencies misinterpreted the Controlled Incident Detection metric question in FY 2010 resulting in inaccurate data reported last year. The definition for this capability area has been revised to clarify the question.

A. Administration Priorities

The Federal cybersecurity defensive posture is constantly shifting because of the relentless dynamic threat environment, emerging technologies, and new vulnerabilities. Many threats can be mitigated by following established cybersecurity best practices, and the FY 2011 FISMA Metrics discussed in the following sections establish baseline security practices as an entry level requirement for all Federal agencies. However, more sophisticated or advanced intruders often search for poor cybersecurity practices and target associated vulnerabilities, and mitigating such threat requires personnel with advanced cybersecurity expertise and awareness of the agency's enterprise security posture. Because cybersecurity is a very important factor for agencies to be able to provide essential services to citizens, in FY 2011 the Administration identified three FISMA priorities. They are defined as:

- Continuous Monitoring;
- Trusted Internet Connection (TIC) capabilities and traffic consolidation; and
- HSPD-12 implementation for logical access control.

These priorities provide emphasis on FISMA metrics that are identified as having the greatest utility in mitigating cybersecurity risks to agency information system.

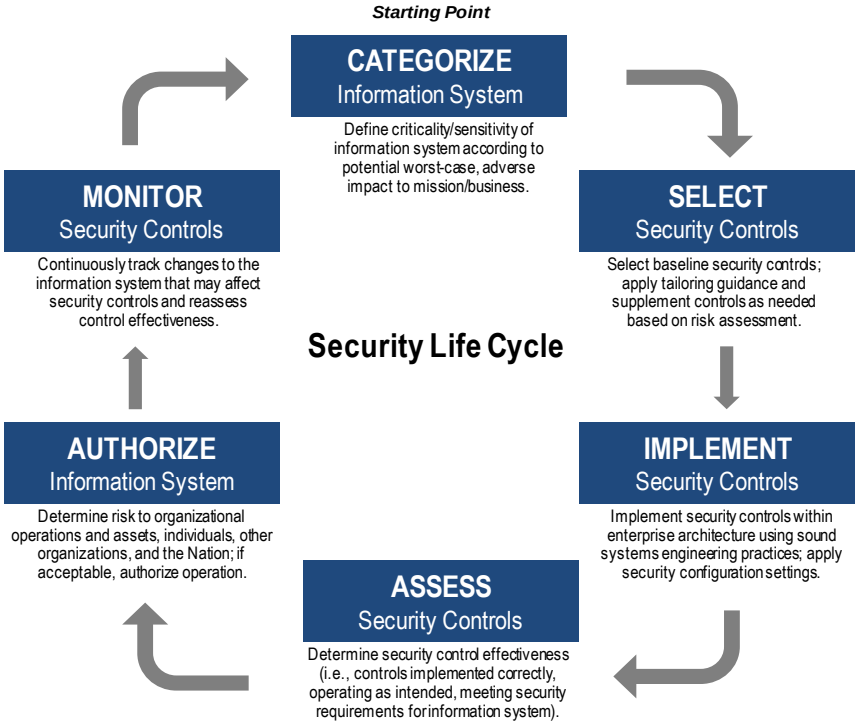
The current status of agency progress and plans for improvement in these capability areas were shared with the President's Management Council to ensure continuous visibility and to emphasize their priority for implementation at the agency level.

Continuous Monitoring

A key element to managing an information security program is having accurate information about security postures, activities and threats. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status. To further these efforts, the National Institute of Standards and Technology (NIST), in February 2010, published the Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*[6], outlining the six-steps Risk Management Framework (RMF). Continuous monitoring is one of the major components within the RMF. Figure 1 below illustrates the RMF processes that provide the foundation for an information system's security life cycle.

[6] Chapter Three of NIST 800-37 Revision 1 describes the six steps of the Risk Management Framework. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Figure 1. Risk Management Framework Overview



In today's environment of widespread cyber-intrusions, advanced persistent threats, and insider threats, it is essential to have real-time accurate knowledge of agencies enterprise IT overall security posture. A agencies need to constantly know and remain aware of their enterprise security status so that responses to external and internal threats can be made swiftly. The FY 2011 continuous monitoring metrics measure the automated ability of agencies to report on their IT assets. Through OMB's directives, agencies are required to collect information from the agencies' security management tools and submit them through automated data feeds directly to CyberScope.

To date, more than 75% of the CFO Act agencies have successfully demonstrated the capability to provide automated data feeds to CyberScope, an increase from only 17% of CFO Act agencies last year. The Administration's goal is for DHS and agencies to leverage this data to better understand and mitigate risk across the Government. The FY 2012 continuous monitoring metrics will focus on continuing to drive the collection of data sets necessary to fully understand and mitigate the risks to our infrastructure.

TIC Security Capabilities and Traffic Consolidation

The Administration's Trusted Internet Connections (TIC) Initiative aims to improve the Federal Government's security posture through the consolidation of external telecommunication connections, by establishing a set of baseline security capabilities through enhanced monitoring and situational awareness of all external network connections.

The purpose of the TIC initiative is to reduce, consolidate, and secure connects to the Federal Government, including those to the Internet. This is accomplished by establishing TIC access portals (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.

Since DHS and the inter-agency group developed the original TIC v1.0 technical reference architecture requirements in 2009, external threats continue to evolve. Through FY2010 and FY2011, DHS worked with an inter-agency group of subject matter experts to update the TIC baseline security capabilities. TICAPs and Managed Trusted Internet Protocal Services (MTIPS) providers are now implementing TIC v2.0 through FY2012, in coordination with other network changes needed to support Internet Protocol version 6 (IPv6).

In FY 2011, DHS began development efforts for the NCPS EINSTEIN 3 capability, which 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, the TIC Initiative aims to further improve the agencies' security posture and incident response capabilities.

Homeland Security Presidential Directive 12 (HSPD-12)

The 2009 *Cyberspace Policy Review*, issued at the direction of the President, and the President's Budget for FY 2011 highlighted the importance of identity management in protecting the nation's infrastructure. Homeland Security Presidential Directive (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 Personal Identity Verification (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.[7]

In February 2011, OMB and DHS issued Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification

[7] HSPD-12, paragraph 4, requires that agencies use the identification standard to the maximum extent practicable; therefore, exceptions to using PIV credentials must be justified by extenuating circumstances (e.g. system is in the process of being decommissioned.)

Standard for Federal Employees and Contractors[8]." This memorandum outlines 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, by March 31, 2011, 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.

To support this effort, the Federal CIO Council and OMB developed a segment architecture[9] for identity, credential, and access management (ICAM). This common government-wide architecture, released in November 2009, supports the enablement of ICAM systems, policies, and processes to facilitate business between the Government and its business partners and constituents. The architecture provides Federal agencies with a consistent approach for planning and executing ICAM 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.

In December 2011, the *Federal Identity, Credential and Access Management Roadmap and Implementation Guidance Version 2.0* was released which provides additional guidance on topics such as modernizing physical and logical access control systems to leverage Personal Identity Verification (PIV) credentials. Additionally, the Department of Commerce National Institute of Standards and Technology (NIST) is in the process of revising the HSPD-12 standard, FIPS 201[10], to address the integration of PIV credentials with mobile devices and advances in technology. In response to demand for improved digital identification from the private sector, other levels of government, and the general public, the Administration also released the National Strategy for Trusted Identities in cyberspace (NSTIC) in April 2011. The NSTIC promotes a public-private collaboration to develop an optional and voluntary privacy-enhancing infrastructure for better online authentication and identification. The NSTIC outlines an approach for the executive branch to catalyze and facilitate the private sector's development of this online identity environment, in

---

[8] 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

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

[10] 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.

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 ICAM roadmap will continue to guide Federal efforts, while the NSTIC will extend the principles of the ICAM activities to provide the framework for the broader public and private, national and international efforts.

B. CyberStat

In FY 2011, DHS provided agencies with their current status cybersecurity posture, based on CyberScope data, and asked agencies to complete a Plan of Action for improving specific cybersecurity capabilities. Agencies were asked for maturity targets to demonstrate quarterly and fiscal year targets in working towards implementation maturity through FY 2012.

Equipped with the reporting results from CyberScope and agency Plans of Action, DHS, along with OMB and NSS, conducted the first CyberStat reviews of selected Agencies. These CyberStat reviews were face-to-face, evidence-based meetings to ensure agencies were accountable for their cybersecurity posture and at the same time assist them in developing focused strategies for improving information security posture. The CyberStat reviews were designed to provide the opportunity for agencies to identify the cybersecurity capability areas where they may be facing implementation maturity roadblocks (e.g. technology, organizational culture, internal process, or human capital/financial resource challenges) and jointly identify potential options for mitigating any barriers.

Additionally, DHS interviewed agencies' CIO and CISO on their agency's security posture. Each interview session had three distinct goals: (1) assessing the agency's FISMA compliance and challenges, (2) identifying security best practices and raising awareness of FISMA reporting requirements, and (3) establishing meaningful dialogue with the agency's senior leadership. Together with the CIO and the CISO interviews, the CyberStat reviews presented the opportunity to communicate to agencies the Administration's FISMA priorities of: continuous monitoring, TIC compliance and traffic consolidation, and HSPD-12 implementation and allowed DHS to provide support and reinforce accountability for agency improvements of their cybersecurity posture.

C. Information Security Workforce

To protect and defend the nation's digital information and infrastructure, the United States must encourage cybersecurity competencies across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats. Forward-thinking agencies have been developing their own cybersecurity workforces, and this unprecedented growth has outpaced the government's ability to standardize and support expectations and norms that permit effective cross-government cybersecurity workforce efforts.

Until today, there has been little consistency in how cybersecurity work is defined or described throughout the Federal Government and 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. Consequently, establishing and using a common lexicon and taxonomy for cybersecurity work and workers is not merely desirable, but critical to the Federal Government's cybersecurity mission. Given these challenges, the following actions have been undertaken.[11]

- The IT Workforce Committee of the Federal Chief Information Officers (CIO) Council launched the Cybersecurity Workforce Development initiative in late 2008. 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 on the CIO.gov website in December 2011. The matrices are intended to give Federal IT departments and agencies a common framework for describing competencies/skills, education, experience, credentials and 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 guide is broadly written to assist line managers, business unit leaders, and hiring managers. The guide is also intended to help these agency stakeholders partner with human capital professionals as they engage in workforce development activities throughout the employment lifecycle. As agency stakeholders strive to attract, hire, train, develop, and deploy people in these professions, this guide will assist them in using best practices to meet these objectives. Therefore, the guide endeavors to provide an initial foundation to help agencies create highly trained workforces with deep leadership benches and advanced technical expertise.
- Two Executive Branch initiatives, in 2008 and 2010, led to the founding of the National Initiative for Cybersecurity Education (NICE) as a Federal and nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Since late 2010, the National Institute of Standards and Technology (NIST), through NICE, has developed a taxonomy of Cybersecurity roles. Currently out for public comment and available in Quarter 2 FY 2012 for adoption through FYs 2012 and 2013, the NICE framework organizes cybersecurity into seven high-level categories, each comprising a subset of 31 specialty areas. Nearly one thousand task, knowledge, skill, and ability descriptions detail the composition of these areas. This organizing structure is based on extensive job analyses and combines work and workers that share common major functions, regardless of actual job titles or other occupational terms.

[11] As stated in the Nice Cybersecurity Workforce Framework at: http://csrc.nist.gov/nice/framework/documents/NICE-Cybersecurity-Workforce-Framework-Summary-Booklet.pdf

The Federal CIO Council and NICE have partnered in their efforts to provide Federal agencies with the tools they need to adopt and implement the NICE Cybersecurity Workforce Framework. This Framework is coordinated with the Office of Personnel Management's February 2011 competency model for the four most common job series used by cybersecurity professionals and puts forth a working taxonomy and common lexicon that can be overlaid onto any organization's existing occupational structure. It has been developed with input from a broad cross-section of sources in government, academia, professional and non-profit organizations, and private industry. It is intended to be comprehensive, but flexible, allowing organizations to adapt its content to their human capital and workforce planning needs. The Framework expedites and gives much-needed, critically required rigor to, for example, workforce baselining, gap analysis, training catalogs, and professional development resources.

III. Security Incidents and Response in the Federal Government

The United States Computer Emergency Readiness Team (US-CERT) receives computer security incident[12] reports from the Federal Government, State/Local governments, commercial enterprises, U.S. citizens and international Computer Security Incident Response Teams (CSIRTs). During FY 2011, US-CERT processed 107,655 incidents as categorized in Figure 2.[13]

Figure 2. Summary of Total Incidents Reported to US CERT in FY 2011

Phishing	55,153	51.2%
Virus/Trojan/Worm/Logic Bomb	8,236	7.7%
Malicious Web Site	6,795	6.3%
Non Cyber	9,652	9.0%
Policy Violation	7,927	7.4%
Equipment Theft/Loss	6,635	6.2%
Suspicious Network Activity	3,527	3.3%
Attempted Access	863	0.8%
Social Engineering	2,573	2.4%
Others	6,294	5.8%
Total	**107,655**	**100.0%**

The incident data revealed the following trends:

- While numerous malicious campaigns impacted the Federal Government, private sector partner organizations, and the general public alike, the total number of reported incidents impacting the Federal Government increased by approximately 5% from FY 2010 while the number of reported incidents from all sectors combined increased by less than 1% for the same period.
    - In FY 2010, US-CERT received a total of 107,439 reports, of which 41,776 of impacted Federal Government departments and agencies.
    - In FY 2011, US-CERT received a total of 107,655 reports, of which 43,889 of impacted Federal Government departments and agencies.

[12] 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.
[13] For information on incident categories, refer to the US-CERT website at: http://www.us-cert.gov/.

- Malicious code continues to be the most widely reported incident type across the Federal Government. As indicated in Table 2, which includes a breakout of incidents reported to US-CERT by Federal agencies in FY 2011, malicious code accounted for 27% of total incidents reported by Federal agencies:

Table 2. Incidents Reported to US-CERT by Federal Agencies in FY 2011

Incidents Category	# of Incidents	% of Total Incidents
Unauthorized Access	6,985	15.9%
Denial of Service	30	0.1%
Malicious Code	11,626	26.5%
Improper Usage	8,416	19.2%
Scans, Probes, and Attempted Access	2,942	6.7%
Under Investigation / Other	13,890	31.6%
Total	43,889	100.0%

The Federal Government continues taking significant measures to better identify and respond to security incidents when they occur. US-CERT issued multiple products to Federal and private sector partners to help prevent and mitigate attack. These products often included information gathered through analysis of suspicious traffic detected via the Einstein system.

US-CERT releases Early Warning and Indicator Notices (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 Security Awareness Reports (SARs) and followed up with impacted agencies.

In addition to EWINs, US-CERT issues weekly Department/Agency Cyber Activity Reports (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.

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 moved from metrics with a compliance driven security focus to performance and outcome-based metrics. The information security performance metrics were designed to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels. The FY 2010 metrics were used to gain greater insight into the security posture of individual Federal agencies as well as establishing an initial government-wide baseline on the cybersecurity posture of the Federal enterprise. The baseline represented the agencies' implementation maturity posture with respect to the security capability areas measured through the metrics asked in CyberScope.

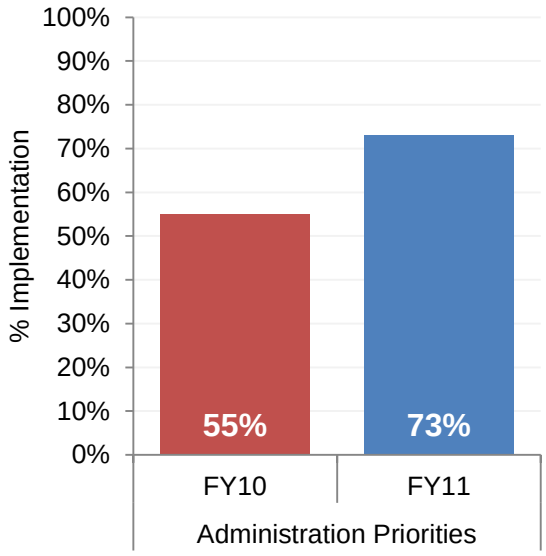
FY 2011 continued along this path with additional security performance measures and expanded metrics around continuous monitoring. The metrics, developed with insight from US-CERT incident information and Intelligence threat data, address key issues for Federal information security. The metrics are tactical, measurable on an ordinal scale, and can be used to drive agency action. With a baseline established, FY 2011 FISMA reporting allows for the measurement of progress in multiple security capability areas both within agencies and across the Federal civilian landscape. Where agencies require improvement in particular areas, the CyberScope and CyberStat processes, discussed in Section II, will be leveraged to assist in improving agency performance.

Additionally, 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 NIST Special Publication 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) implementation costs. While agencies did report some cost information last year, this reporting cycle represents the second year that detailed security cost information has been officially incorporated into agency budget submissions.

A. Information Security Metrics

The following sections highlight the FISMA metrics for the three Administration priorities discussed in Section II, as well as other important security metrics for FY 2011. All data are as reported by agencies with the exception of TIC and Domain Name System Security Extensions (DNSSEC) data which are validated values obtained through compliance scans and on-site assessments conducted by DHS. The Administation FISMA priorities: automated continuous monitoring; TIC security capabilities and traffic consolidation; and HSPD-12 implementation for logical access, detailed in Section 1.A., have shown an overall improvement from 55% in FY 2010 to 73% in FY 2011. The improvement is shown in Figure 3.

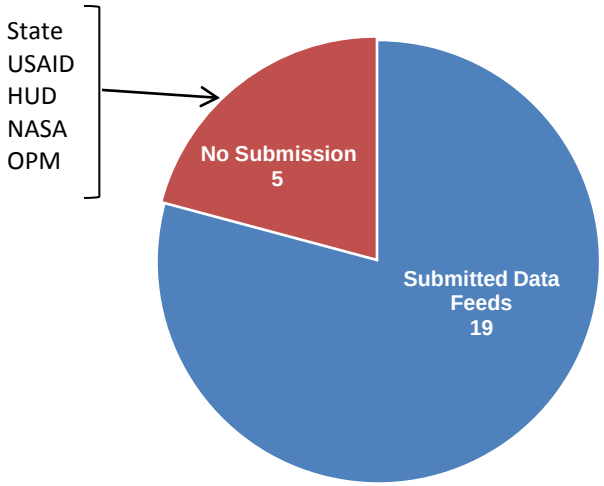
Figure 3. Implementation Percentage of Administration FISMA Priorities in FY 2010 and FY 2011



Continuous Monitoring

In FY 2010, only four agencies submitted automated data feeds to CyberScope. In contrast to FY 2010, 19 out of 24 agencies have successfully submitted automated data feeds in FY 2011. This is a 63% increase in automated reporting capability.

Figure 4. Number of Agencies Submitting Automated Datafeeds to CyberScope



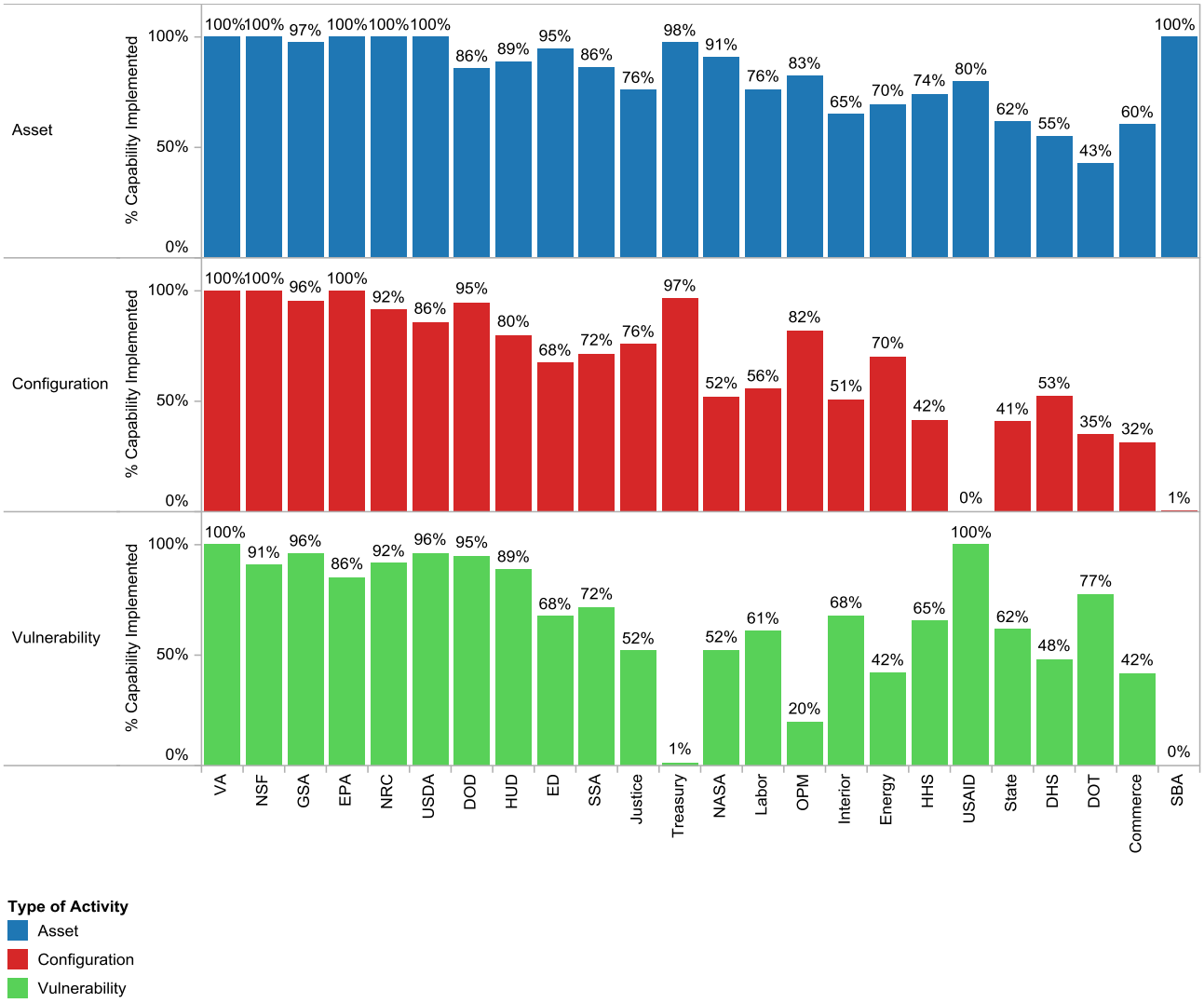
In FY 2011, agency implementation of automated continuous monitoring capabilities rose to 78%, as compared to 56% in FY 2010. All three data feeds (i.e. IT asset inventory, system configuration, and vulnerability management) have provided insight into the number of systems that are being managed under automated asset, configuration, and vulnerability management. Two agency specific

success stories are the Department of Veterans Affairs and the Environmental Protection Agency which went from respective averages of 17% and 26% coverage in FY10 for continuous monitoring to averages of 100% and 95% of systems managed in all three components of continuous monitoring. Not only did the percentage of managed assets rise, but so did the ability of agencies to automate the submission of managed data to CyberScope. 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 2010 agencies reported automated inventory capturing with a success rate at 66%, but in FY 2011 the success rate has increased to 80%.

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 2010, agencies reported that the automated configuration management capability was at the 50% level, but this level had since increased to 78% in FY 2011.

Agencies also made 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 2010, 51% of assets were being managed with an automated vulnerability management capability. At present, analysis of the vulnerability management capability across the government shows 77% 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. Figure 5 illustrates the percentage of IT assets with automated access to asset inventory, configuration management, and vulnerability management information by agency.

Figure 5. Percentage of Continuous Monitoring Capabilities Reported by Agencies

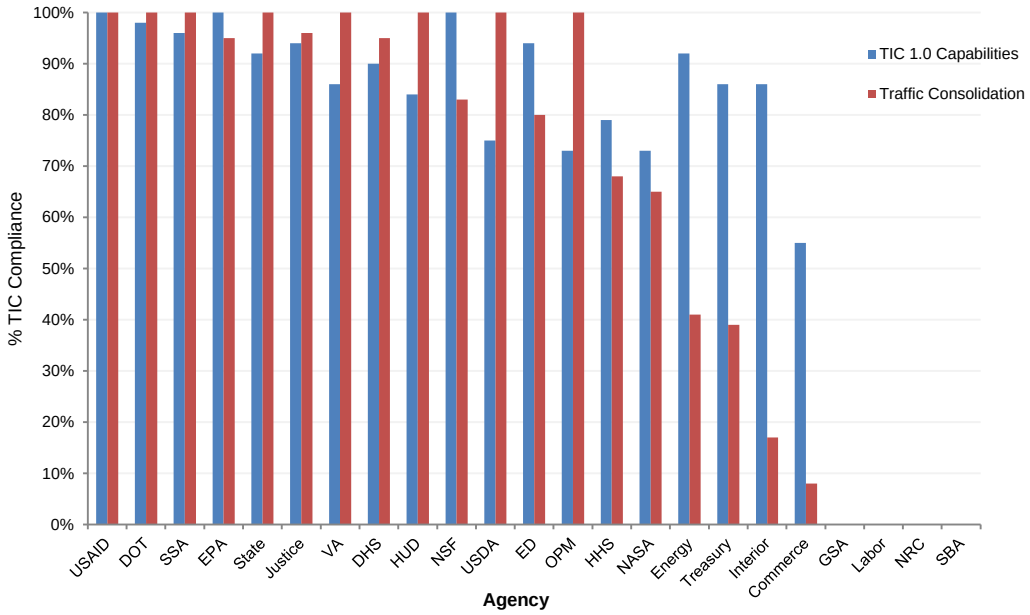


Trusted Internet Connections (TIC) Security Capabilities and Traffic Consolidation

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 who 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 v. 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 48% in FY 2010 to 85% in FY 2011for the 18 assessed TICAPs, and to 27% for the 42 self identified agencies seeking vendor-provided MTIPS The implementation of TIC Reference Architecture v.1.0 critical security capabilities also increased

from 60% in FY 2010 to 85% in FY 2011, though one agency and one MTIPS provider remained to be assessed. Figure 6 illustrates percentage ofTIC security capabilities and traffic consolidation as implemented by agencies.

Figure 6. Percentage of TIC Security Capabilities and Traffic Consolidation Implemented by Agencies



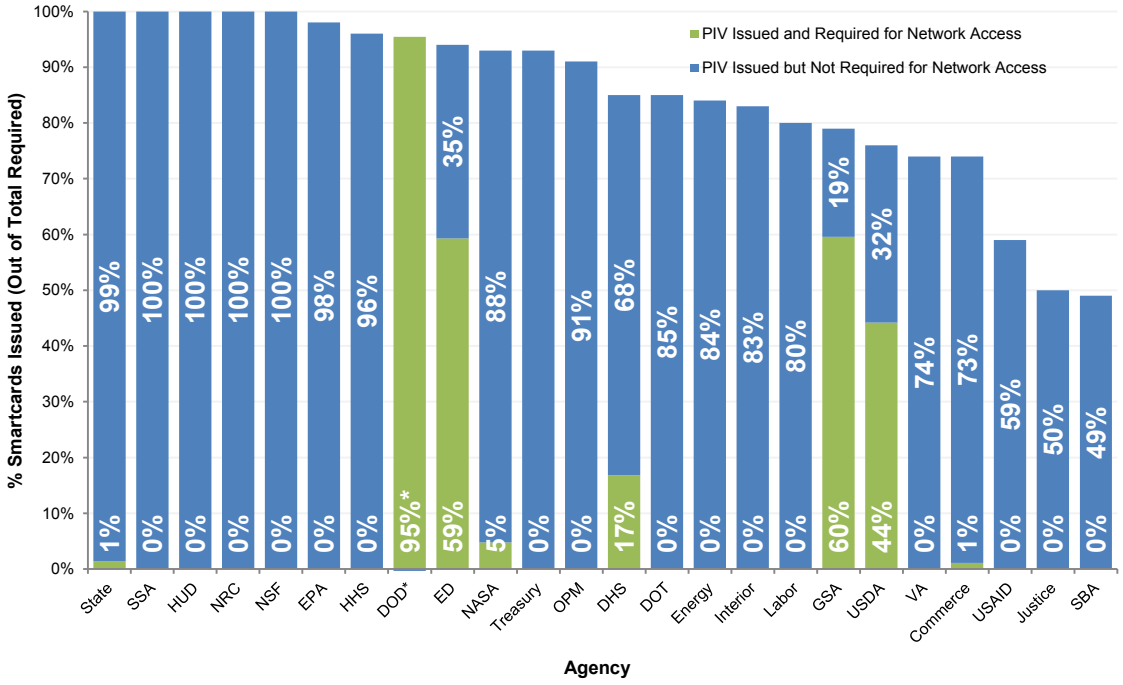
Homeland Security Presidential Directive 12 (HSPD-12)

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, 2011, agencies reported that 89% 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 7 shows, by agency, the issuance progress and percentage of user accounts that require PIV cards for access to the agency's networks.

The FY 2011 FISMA metrics data indicates that 66% of government user accounts are configured to require PIV cards to authenticate to agencies' networks, up from 55% in FY 2010. The increase of 11% was attributable to several agencies which made significant strides in HSPD-12 implementation to include the Department of Education which increased 59% in PIV authentication usage in FY 2011. An additional 22% of user accounts are configured to optionally use PIV cards. Overall, most agencies continued to report little, if any, progress from the previous year for mandatory PIV card usage. At this time last year, only two agencies reported more than 3% of user accounts were required to use PIV cards for network access. In FY 2011 six agencies reported that

5% or more of user accounts required PIV cards for authentication, with four of those agencies at 44% or better. The remaining 18 agencies reported between 1% and 0% of employees were required to use their PIV cards to authenticate to the agency network.

Figure 7. Smartcard Issuance Progress and Percentage of User Accounts that Require the Use of PIV Cards for Network Access Reported by Agencies

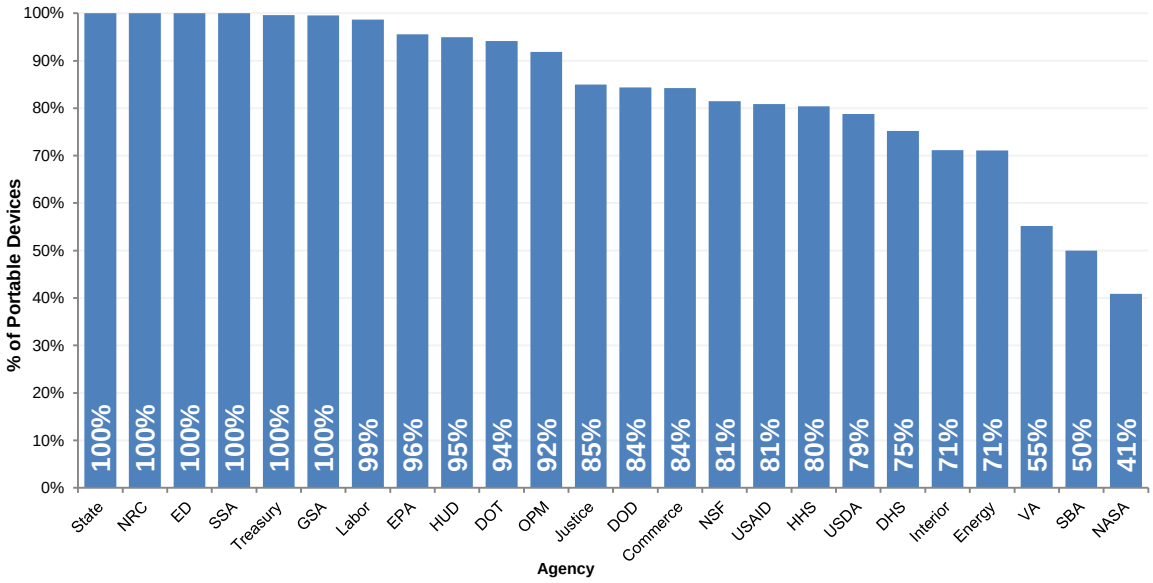


* All PIV card issuance percentages are from September 2011, and PIV card usage percentages are from November 2011. DOD reported 92% PIV card issuance, and 95% PIV card usage for network access.

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. Improving on last year's metric, FY 2011 captured the encryption percentage of all portable devices to include laptops, netbooks, tablet-type computers, Blackberries, smartphones, USB devices and other mobile devices. Agencies have reported continued progress in implementing this capability. In FY 2010 the reported government-wide average was 54%, but in FY 2011 the government-wide average is 83% with 11 agencies achieved above 90% completion.Portable devices are a primary source for the loss of sensitive data because they move outside the protection of physical and electronic barriers that protect other hardware assets. 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 8 shows the percentage of agency portable devices with FIPS 140-2 validated encryption.

Figure 8. Percentage of Portable Devices with Encryption Reported by Agencies

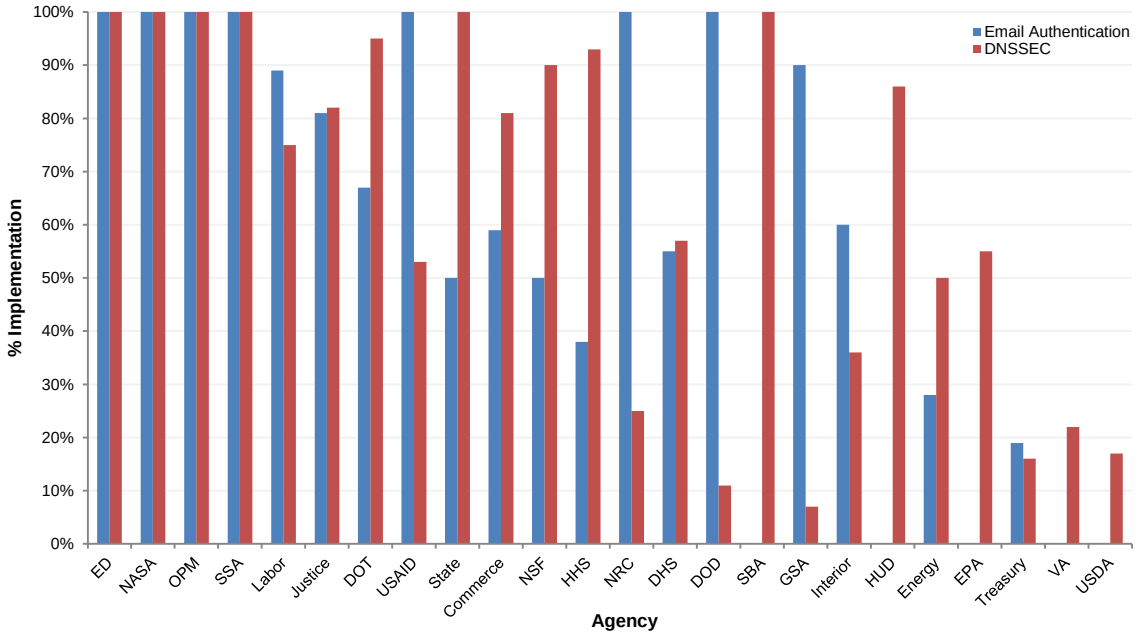


Domain Name System Security Extensions (DNSSEC) Implementation and Email Validation

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.

For FY 2010 and FY 2011, the deployment of DNSSEC was tracked by both the self-reporting of the agencies (traditional FISMA reporting) and through an automated compliance scan of government domains. The two reports revealed very different results highlighting the accuracy and need for automated tools. With the configuration and deployment of automated tools, agencies can quickly, reliably, and accurately garner the information necessary to improve and maintain their security posture. Figure 9 shows by agency the DNSSEC deployment and percentage of email systems with sender verification technologies. Six agencies, Department of Education, National Air and Space Administration, Office of Personnel Management, Social Security Administration, Department of State, and Small Business Administration had 100% signed second level domains for DNSSEC.

Figure 9. Percentage of Validated DNSSEC and Email Sender Varification Reported by Agencies



Agencies reported progress from FY 2010 to FY 2011 in this capability area, with the government-wide compliance rate at 35% in FY 2010 to 65% in FY 2011. The DNSSEC values were measured using an automated tool developed by DHS. To encourage increased adoption of DNSSEC, DHS in conjuction with ISIMC formed a tiger team to focus efforts on this challenge. The goal of the tiger team was to improve the DNSSEC and email authentication outcome metrics across agencies by focusing efforts on critical barriers to implementation and deliverables that can assist in implementation. The tiger team held multiple government-wide meetings of Subject Matter Experts (SMEs) to collect and share best practices and lessons learned, and compiled those inputs into the soon-to-be-released document, *Considerations and Lessons Learned for Federal Agency Implementation of DNS Security Extensions and E-mail Authentication*. DHS also created and released several tools for DNSSEC and email authentication testing, and hosted multiple classes and training for technical implementation.

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 reasonable assurance that the messages they receive are authentic government correspondence and arrive intact. In addition, fraudulent email sent to Federal agencies is a significant security risk for Federal systems. A key objectives is to increase the level of trust in email authenticity. By coupling anti-spoofing technologies with sender verification techniques, the security of email can be improved across the board. In FY 2011 DHS published the *Email Gateway Technical Reference Architecture* to facilitate agency implementation of these crucial technologies. Agencies were asked to report the percentage of Agency email systems that implemented sender

verification (anti-spoofing) technologies when sending messages to/from government agencies. In FY 2010 the government-wide average was reported at 46% for email validation. The government-wide average has increased to 58% in FY 2011 with several agencies achieving 100%. Email protections are directed to reduce the number of phishing attacks, which currently represent a high risk threat.

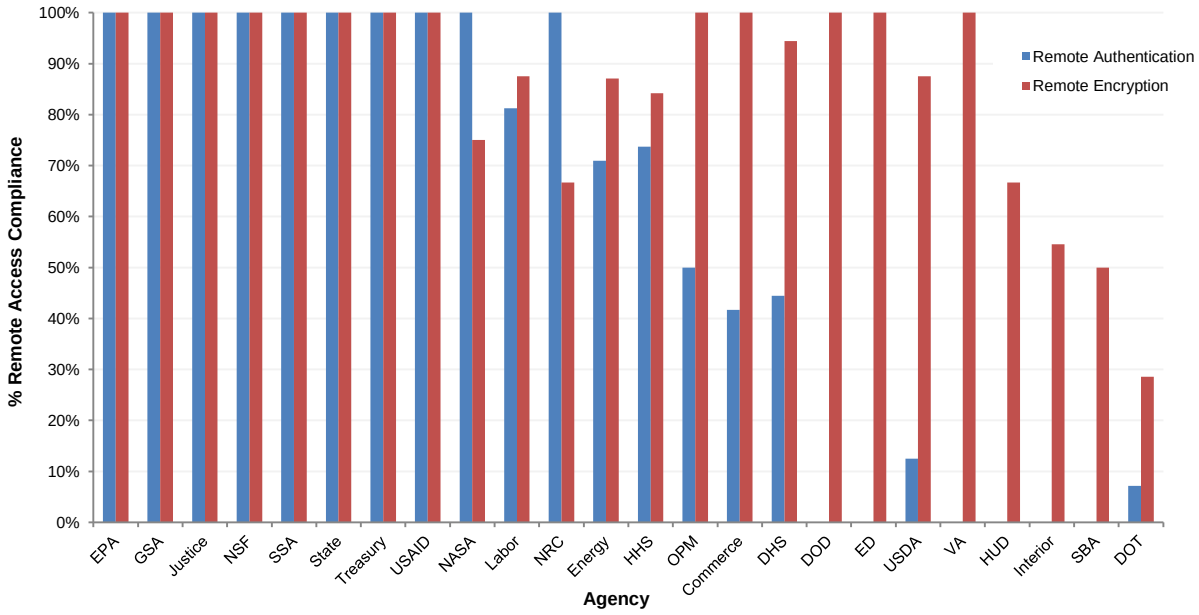
Remote Access

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 for the number of agency remote access connection methods that still used userID and password as the sole method of authentication. Agencies are moving towards two-factor authentication and many agencies are decommissioning userID and password methods of access. However, several CFO agencies require improvements in their remote access authentication with some agencies reporting that userID and password are still valid authentication for all their remote access methods. Across the Government 52% of remote access methods disallow the use of userID and password combinations as a method of authentication, consistent with FY 2010.

Agencies were asked how many of their remote access methods utilized FIPS 140-2 validated cryptographic modules. Remote Access Encryption showed improvements with an average of 83% for CFO agencies up from 72% in FY 2010. More than half of the agencies reported 100% in this capability.

Overall, significant gaps exist in providing robust, secure remote access options. In many cases the gaps are related to other capability areas that when matured, will carry over to this capability area. However, given the growing importance of telework and the lack of robust implementations apparent across the agencies, in FY 2012, DHS will be publishing a reference architecture outlining designs for providing secure remote access/telework options. Adequate control of remote connections is a critical part of boundary protection because these connections are beyond physical security controls. Remote access connections need compensating controls to ensure that only properly identified and authenticated users gain access, and that the connections prevent hijacking by others. Figure 10 shows the percentage of remote access connection methods, by agency, that require more than just userID and password authentication in addition to requiring FIPS 140-2 encryption for connections.

Figure 10. Percentage of Remote Access Methods Disallowing UserID and Password for Authentication and Requiring Remote Access Encryption Reported by Agencies

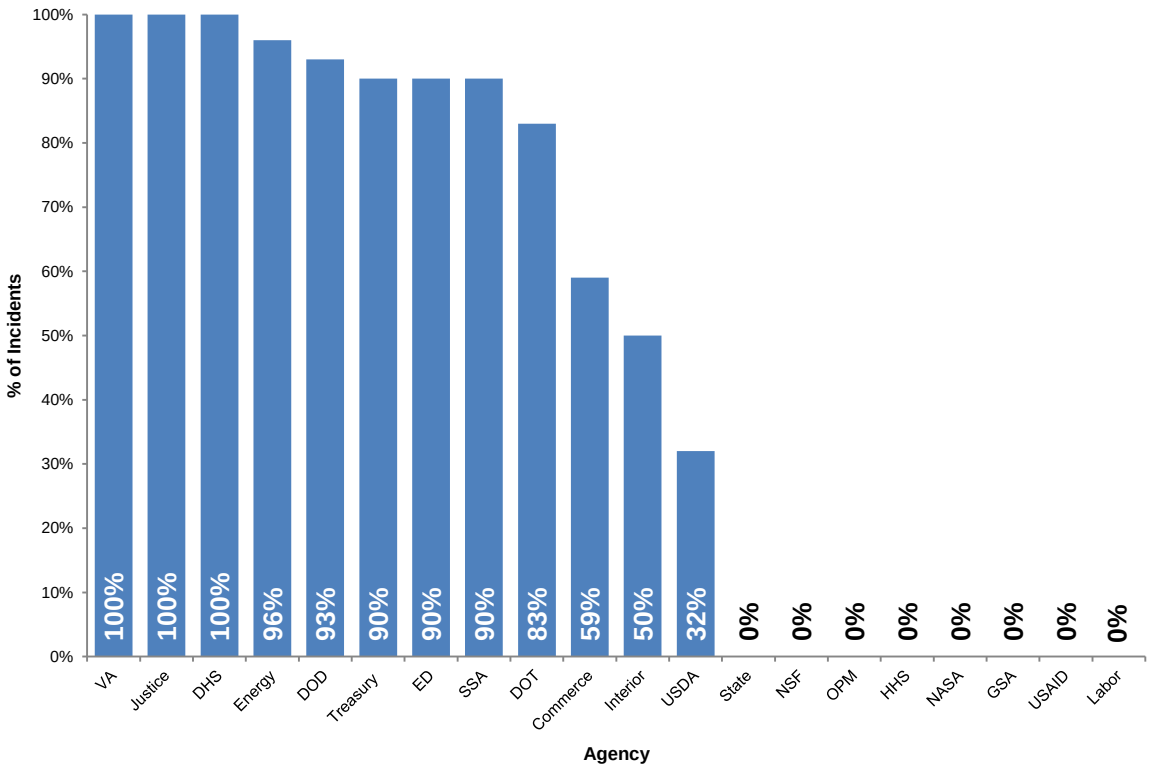


Controlled Incident Detection

The incident management capability must be coupled with a highly skilled and trained set of technical resources. The ability to accurately assess this capability will keep improving as it matures. In addition, US-CERT is making significant strides in increasing communication with agency Network Operation Centers (NOCs) and Security Operation Centers (SOCs). 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. This also provides useful information to the risk management process to determine the level of cyber resources to invest in incident detection and response.

For agencies conducting controlled penetration tests, the NOC/SOC was 49% effective at detecting incidents, with several agencies reporting the detection of incidences by other business processes. This capability dropped from 70% in FY 2010. This continues to highlight the need for automated data feeds based on common definitions and established standards. Figure 11 illustrates the percentage of controlled penetration testing events detected by agencies.

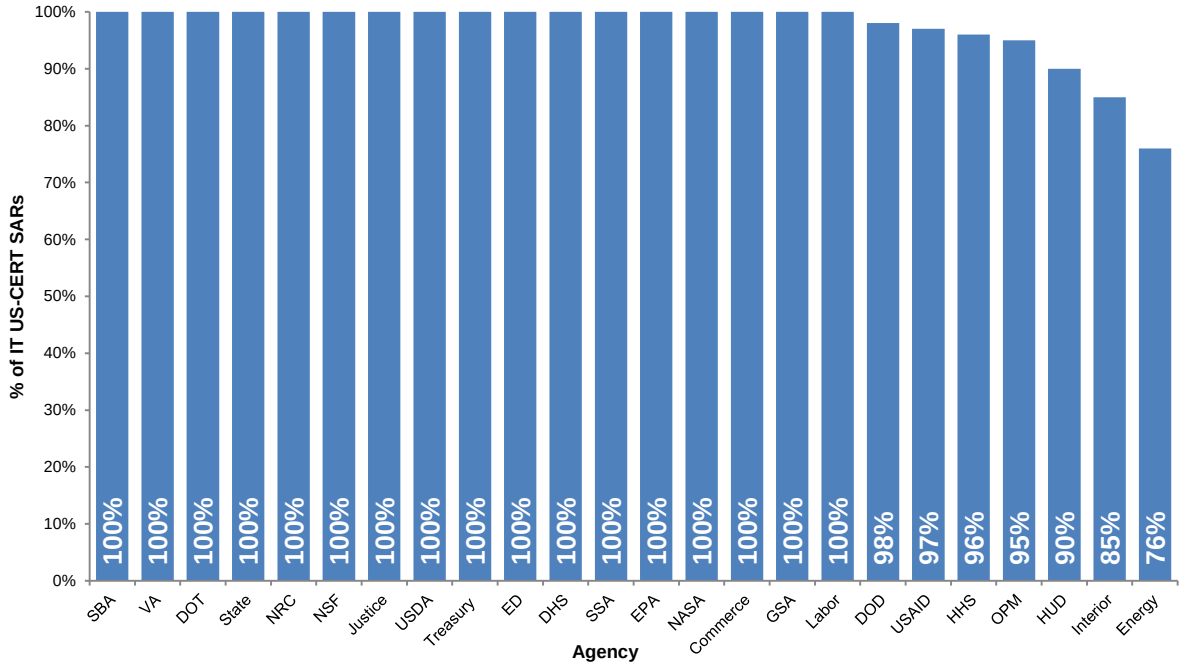
Figure 11. Percentage of Controlled Incident Detection as Reported by Agencies



USCERT SAR Remediation

US-CERT Security Awareness Reports (SARs) communicate broad assessments of threats and inform departments/agencies of actionable recommendations for monitoring and responding to suspicious activity. Agencies were asked for the percentage of US-CERT SARs, or Information Assurance Vulnerability Alerts for DOD, which had been acted upon in FY 2011. As indicated below in Figure 12, agencies reported having remediated 97% of vulnerabilities described in US-CERT SARs, an improvement of 7% from FY 2010.

Figure 12. Percentage of US-CERT SARS Remediated Reported by Agencies



Security Training

Training continues to hold significant importance in addressing challenges associated with protecting our networks, systems, and data. One of the greatest threats is phishing attacks, where a network user responds to a fraudulent message producing a negative impact on confidentiality, integrity, and/or availability of the organization's information. Given the prevalence of phishing attacks and the continual evolution of adversary tactics, techniques, and procedures, the frequency and effectiveness with which users and security professionals receive training and education must be increased and the content continually refreshed to include new and creative training mechanisms to communicate this important and evolving threat.

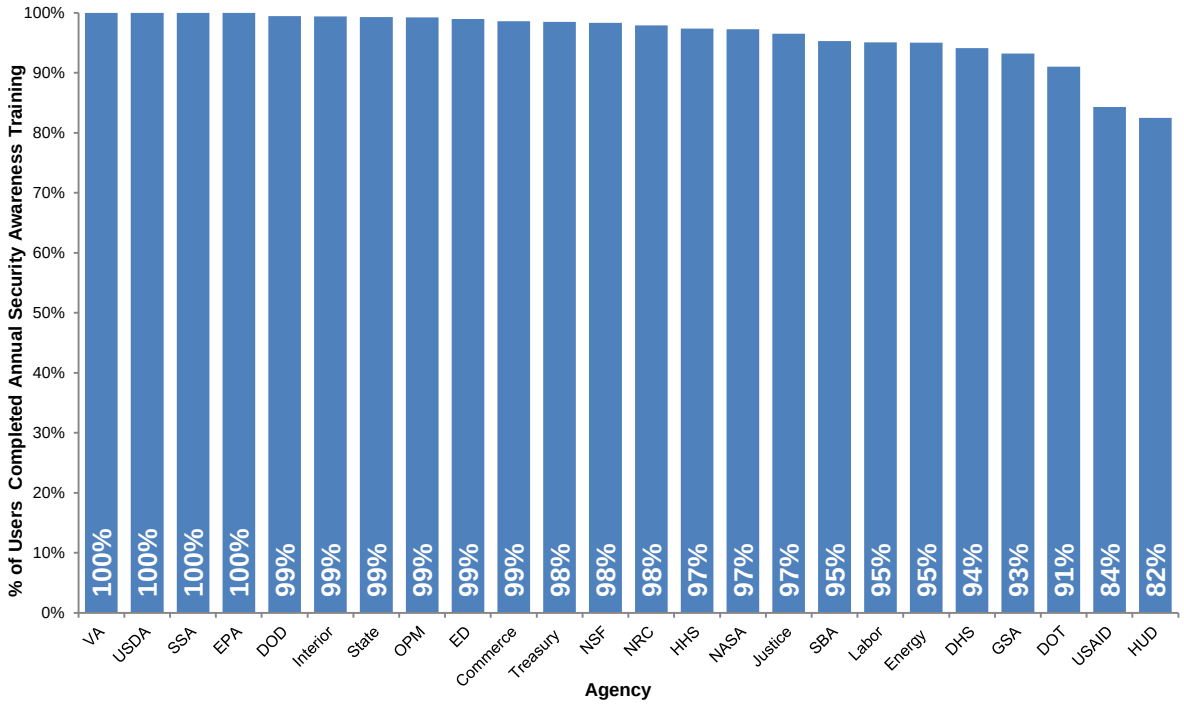
Agencies updated the content of their security training with greater frequency in FY 2011. Virtually all agency training includes the security risks of wireless technologies along with awareness of security policies and procedures for mobile devices. Every agency now includes content on how to recognize and avoid phishing attacks in their annual security awareness training and 60% of the agencies reinforce this with agency-sponsored phishing attack exercises to train users on the correct response.

Agencies are generally meeting the annual requirement for cybersecurity awareness training, with more than two thirds providing supplemental security training every quarter, and some, as a best practice, providing daily supplemental security training.

For agency users with network access privileges, 99% were given annual security awareness training, which is up from 92% in FY 2010. Agencies also reported that 83% of new users were

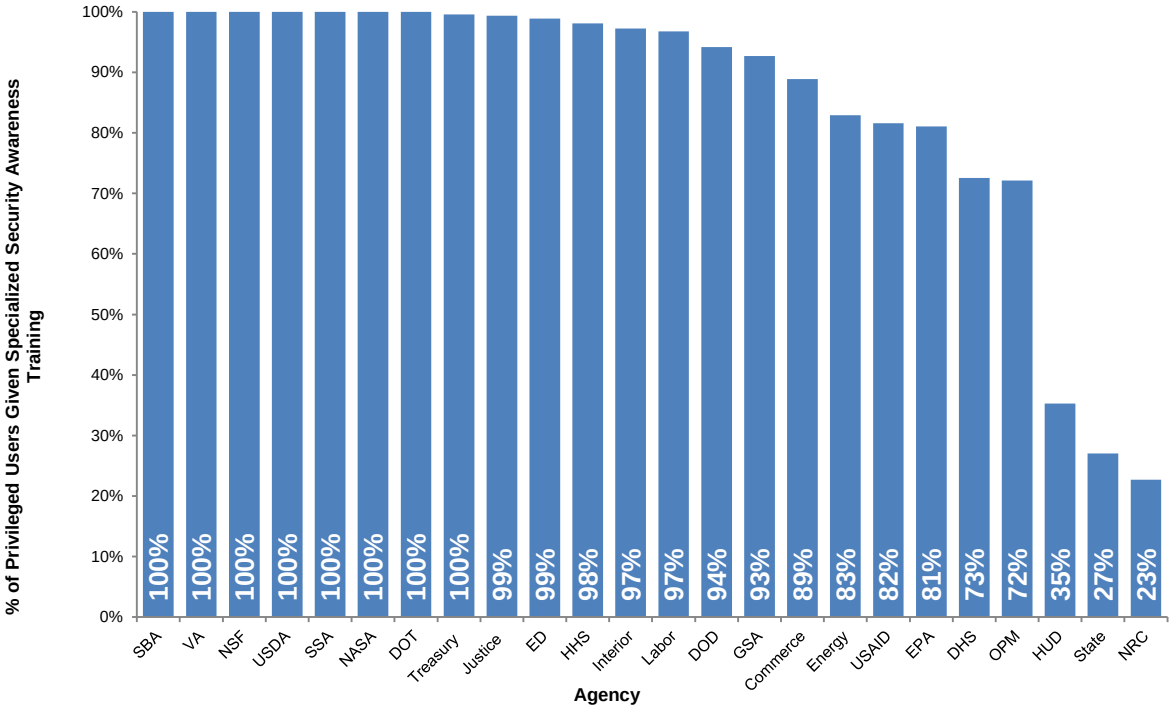
given security awareness training prior to being granted network access. Figure 13 below provides by agency, the percentage of users completing annual security awareness training.

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



Some users have significant security responsibilities, a role where the daily assigned duties reflect an elevated authorized access to systems, data, and environments. 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 with significant security responsibilities that had been given specialized, role-based, security training annually. Specialized cybersecurity training for agency privileged users averages 92% across all Federal agencies in FY 2011, an increase from 88% in FY 2010. 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



B. Information Security Cost Metrics

Securing government's information and information systems is a major responsibility and agencies must devote sufficient resources to ensure that government and citizens' information remain secure. The OMB Exhibit 53B Agency IT Security Portfolio section requires agencies to report IT security cost and budget data. Agencies reported cost information in areas such as IT security testing, security tools, assessment and authorization, training, and personnel.

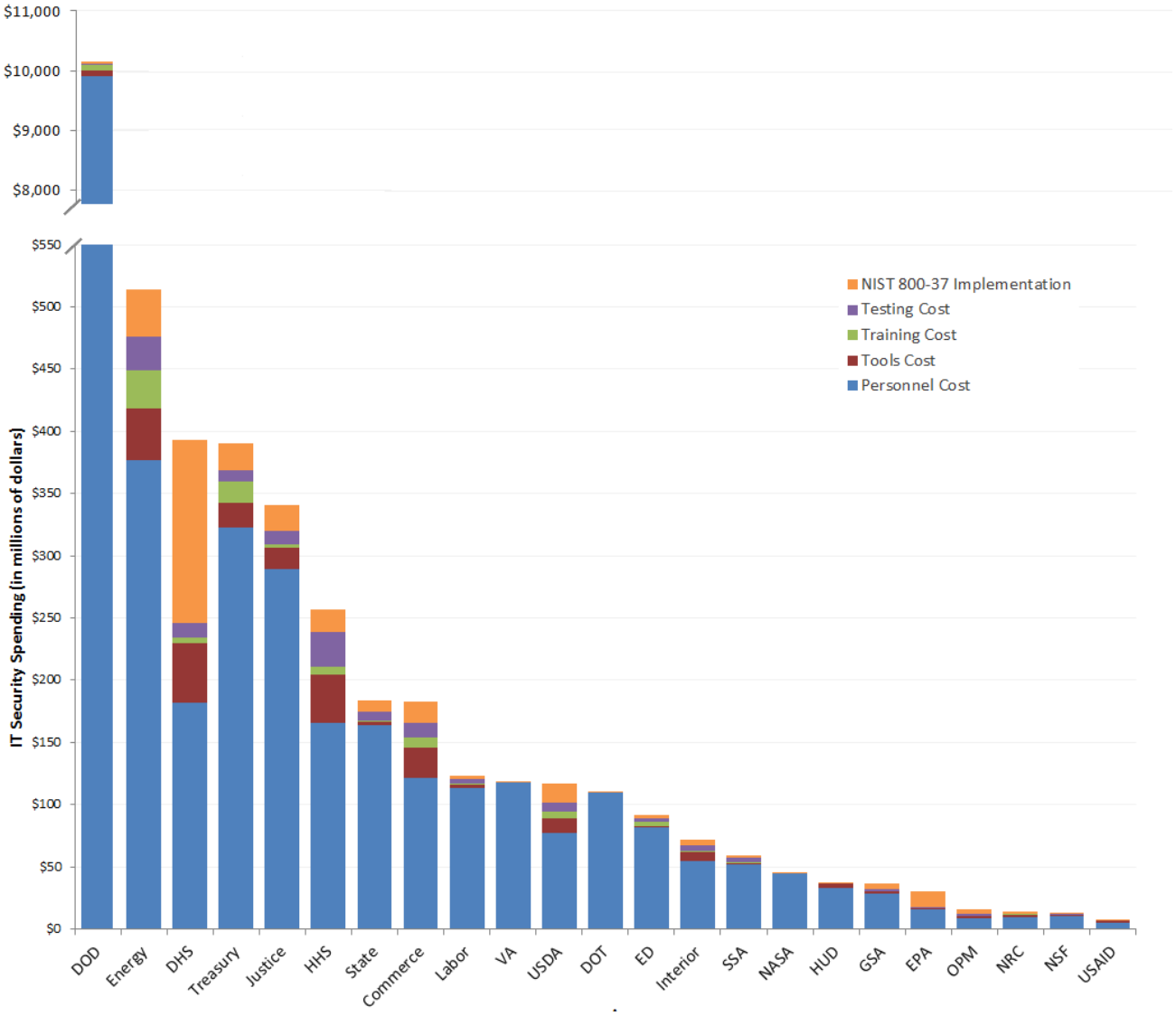
This section of the FISMA report provides the IT security cost analysis based on the Exhibit 53B data for FY 2011.[14]

IT Security Spending by Agency

In FY 2011, the CFO Act agencies reported total IT security spending of $13.3 billion. Figure 15 provides the agency-reported IT security cost by spending category.

[14] The Department of Defense (DOD) stated that they were unable to provide department-wide cost information for security tools. DOD's IT security cost information was not provided in the form of an Exhibit 53B.

Figure 15. IT Security Spending Reported by Agencies



The total IT security cost includes cost categories for direct spending such as costs for security personnel[15], tools, testing, training, and NIST SP 800-37 implementation.

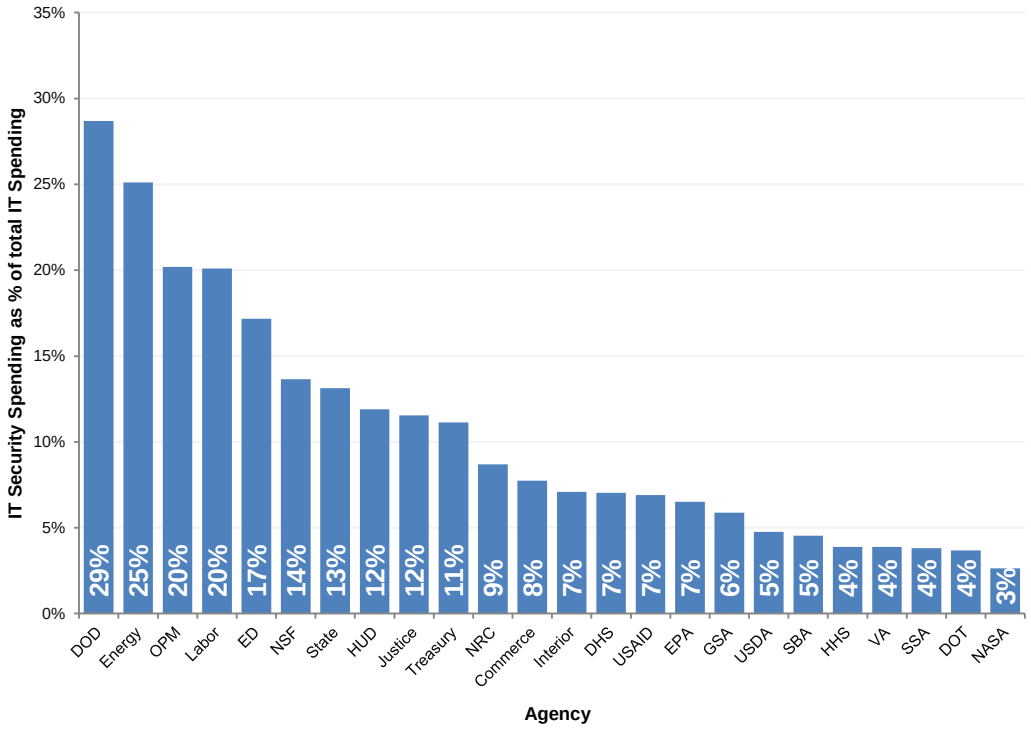
Indirect spending such as mission-related IT security cost is not included. Indirect spending on IT security might include costs for activities such as: security configuration fixes and recovering a compromised system; architecture redesign to enhance security; upgrading existing systems and installing replacement systems that provide more secure capabilities; institutionalizing IT security; and reporting and auditing.

[15] Number of FTEs is different from number of persons. In the U.S. Federal Government, FTE is defined as the number of total hours worked divided by the maximum number of compensable hours in a work year as defined by law. For example, if the work year is defined as 2,080 hours, then one worker occupying a paid full time job all year would consume one FTE. Two persons working for 1,040 hours each would consume one FTE between the two of them.

The indirect costs of IT security are very difficult to separate from other operational and managerial costs. For instance, effective security programs are typically tightly integrated with other activities. However, it should be noted that direct costs are only part of the total IT security costs spent by an agency.

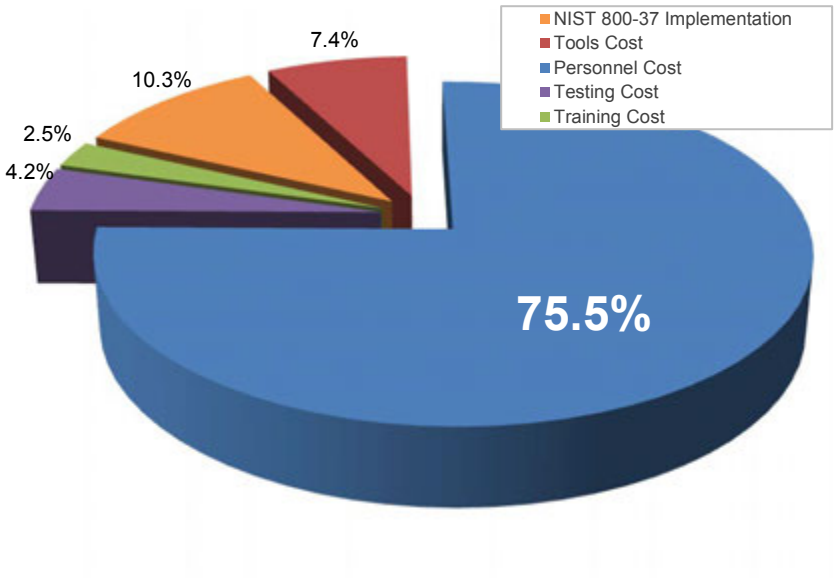
Figure 16 shows the percentage of FY 2011 IT spending that was for IT security. Overall, 18% of agencies' IT spending was spent on IT security. CFO Act agencies spent a range of 3% to 29% of their total IT budget on IT security.

Figure 16. IT Security Spending as a Percentage of Total IT Spending Reported by Agencies



In FY 2011, 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. Non-defense agencies spent 76% of their IT security costs on personnel, as indicated in Figure 17 below.

Figure 17. Percentage Breakout of IT Security Costs by Category Reported by Agencies



Note: The percentages are the average of 23 agencies, excluding Department of Defense.

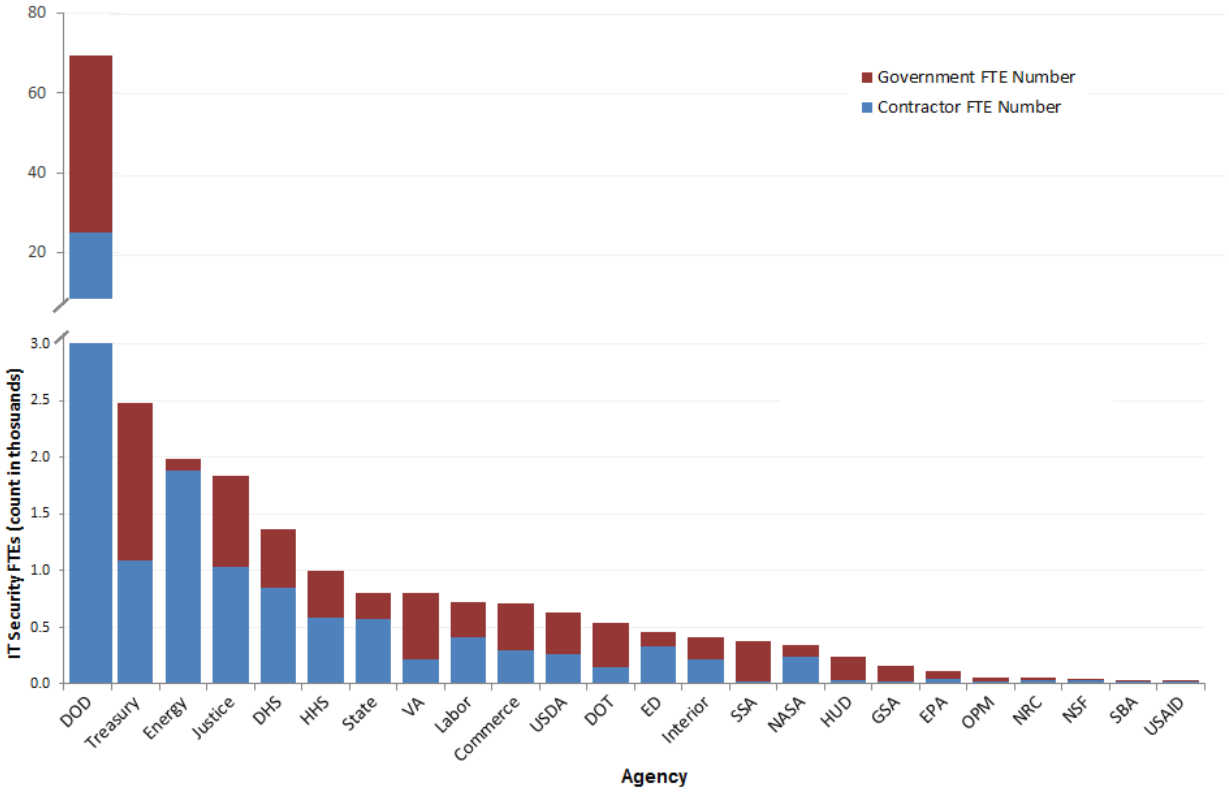
As further indicated by Figure 17 of the reported IT security costs government-wide, agencies spent 7% on security tools, 10% on NIST 800-37 implementation, 4% on security testing, and 3% on security training. NIST 800-37 requires agencies to apply the Risk Management Framework to Federal information systems using a Security Life Cycle Approach, advancing from the previous periodic Certification and Acredidation (C&A) process into the more continuous Security Authorization Process.

The composition of IT security costs indicates that personnel costs continue to be the majority of IT security 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 2011, CFO Act agencies reported a total of 84,426 Full Time Equivalents[16] (FTEs) with major responsibilities in information security. Figure 18 provides a breakout of Total IT Security FTEs by agency.

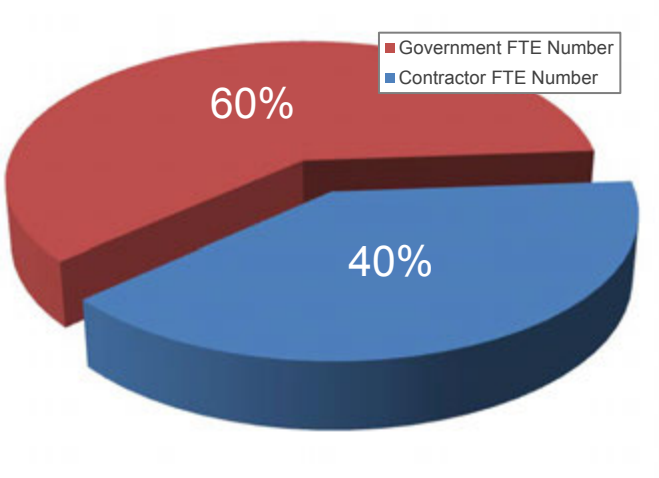
Figure 18. Total IT Security FTEs Reported by Agencies



[16] Number of FTEs is different from number of persons. In the U.S. Federal Government, FTE is defined as the number of total hours worked divided by the maximum number of compensable hours in a work year as defined by law. For example, if the work year is defined as 2,080 hours, then one worker occupying a paid full time job all year would consume one FTE. Two persons working for 1,040 hours each would consume one FTE between the two of them.

Of the total FTEs for the CFO Act agencies, 60% are government FTEs, 40% are contractor FTEs (Figure 18) . This percentage is heavily influenced by DOD's large FTE numbers. DOD's IT security personnel are 64% government FTEs and 36% contractor FTEs. Excluding DOD, 45% of security FTEs are government FTEs, and 55% are contractor FTEs. IT security has consistently been a functional area that depends on talent and technical expertise from industry and commercial sources.

Figure 19. Percentage of Government FTEs Compared to Contractor FTEs



V. Summary of Inspectors General's Findings

Each inspector general (IG) was asked to assess his or her agency's information security programs in the following eleven areas:

- Risk management
- Configuration management
- Incident response and reporting
- Security training
- Plans of actions and milestones (POA&M)
- Remote access management
- Identity and access management
- Continuous monitoring management
- Contingency planning
- Contractor systems
- Security capital planning[17]

IGs were asked to evaluate 127 attributes in each of these eleven areas and determine whether: (1) that the agency had established and maintained a program that was generally consistent with NIST and OMB's FISMA requirements, and included the needed attributes; (2) the agency had established and maintained a program that needed significant improvements; or (3) the agency had not established a program for the area. If an agency's program for a certain security area needed improvements, the IG identified the issues and required improvements from a list of possible problem issues for each of the eleven areas. If an issue and the needed improvement did not appear on the area's list of issues, the IG provided a narrative describing the issue and the needed improvements. IGs could report that a program was generally consistent with requirements, but still mark specific attributes as non-compliant. This possibility was not available in FY 2010 reporting requirements and resulted in a minor modification to 2011's scoring formula.

Table 3 summarizes the results from the IGs of the 24 CFO Act agencies according to cyber security program area. These results indicate that the agencies 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.

[17] Security capital planning was a new metric for FY 2011.

Table 3. Results for CFO Act Agencies, by Cyber Security Area

Cyber Security Program Area	Compliant Program			Needs Improvement			Program Not Implemented		
	FY11	%	FY10	FY11	%	FY10	FY11	%	FY10
Risk Management	8	33	13	16	67	11	0	0	0
Configuration Management	6	25	6	18	75	18	0	0	0
Incident Response and Reporting	16	67	15	8	33	9	0	0	0
Security Training	12	50	7	12	50	17	0	0	0
POA&M	6	25	8	18	75	16	0	0	0
Remote Access Management	13	54	10	11	46	14	0	0	0
Identity and Access Management	6	25	5	18	75	19	0	0	0
Continuous Monitoring Management	9	37	7	12	50	15	3	13	2
Contingency Planning	8	33	8	16	67	16	0	0	0
Contractor Systems	10	42	6	14	58	16	0	0	2
Security Capital Planning	16	67	N/A	8	33	N/A	0	0	N/A

Table 4 provides CFO Act agencies compliance scores. The Department of Defense did not provide sufficient information for scoring. The Nuclear Regulatory Commission, National Science Foundation, and Social Security Administration had compliant programs in place for all eleven areas, although each did identify areas for improvement. The remaining agencies had at least one area that needed significant improvement. Three agencies—the Department of Housing and Urban Development, Office of Personnel Management, and the Agency for International Development—all reported that they did not have continuous monitoring management programs in place. In FY2010, all three of these agencies reported having a continuous monitoring program at least partially in place, while two different agencies reported not having a continuous monitoring program —an indication of gains in some areas and losses in others. Total numbers of areas with deficiencies were used to compute compliance scores. Seven agencies scored over 90 percent compliance, eight scored between 65 and 90 percent compliance, and the remaining eight scored less than 65 percent. The average score across the agencies was 72.8 percent. Nine agencies improved over their FY 2010 scores, with NASA showing the largest gain of 32.1 points. Eleven agencies had scores that were lower that their FY 2010 scores. The United States Agency for International Development had the largest decline of 36.6 points. Three agencies maintained their scores from 2010 within +/- 1 point.

Table 4. CFO Act Agencies' Compliance Scores, Based on IG's Reviews

Agency	FY11 (%)	FY10 (%)	Change
National Science Foundation	98.8	98.9	-(0.1)
Social Security Administration	96.9	100	-(3.1)
Environmental Protection Agency	94.9	99.2	-(4.3)
Nuclear Regulatory Commission	94.8	96.7	-(1.9)
Department of Homeland Security	93.4	92.5	0.9
National Aeronautics and Space Administration	92.9	60.8	32.1
Department of Justice	91.2	85.8	5.4
Department of Energy	84.3	84.6	-(0.3)
General Services Administration	84.2	87.6	-(3.4)
Department of Commerce	81.4	77.9	3.5
Department of the Treasury	79.4	86.4	(-7.0)
Office of Personnel Management	78.6	57.8	20.8
Department of Labor	71.6	44.5	27.1
Small Business Administration	68.7	50.3	18.4
Department of Housing and Urban Development	66.1	87.3	-(21.2)
Department of State	63.2	79.4	-(15.2)
Department of Education	57.5	71.9	-(14.4)
United States Agency for International Development	53.8	90.4	-(36.6)
Department of Veterans Affairs	52.8	57.0	-(4.2)
Department of Health and Human Services	50.9	64.7	-(13.8)
Department of Transportation	44.2	29.8	14.4
Department of the Interior	42.2	24.6	17.6
Department of Agriculture	32.5	13.7	18.8
Department of Defense	N/A	N/A	N/A*

*DOD did not provide the answers with the detail required for scoring in FY 2010 or FY 2011

Additional details on IG's evaluation results can be found in Appendix 1.

VI. Progress in Meeting Key Privacy Performance Measures

Ensuring the privacy of personal information for all Americans remains a top Administration priority, especially as Federal agencies leverage emerging technologies such as cloud computing, mobile computing devices, and social media. The privacy implications in the use of these technologies must be considered, and agencies should collaborate on solutions and best practices to mitigate privacy risks. 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. In addition, Federal agencies will continue to develop and implement policies outlining rules of behavior, detailing training requirements for personnel, and identifying consequences and corrective actions to address non-compliance. Agencies will work with their Senior Agency Officials for Privacy (SAOP) to ensure that all privacy impact assessments and system of records notices are completed and up-to-date. Finally, agencies will continue to implement appropriate data breach response procedures.

As discussed in the sections that follow, the FY 2011 agency FISMA reports indicate improvements in most privacy performance measures despite an increase in the number of systems requiring compliance. There is also a new section on agency use of web management and customization technologies.

Table 5. Status and Progress of Key Privacy Performance Measures

	FY 2009	FY 2010	FY 2011
Number of systems containing information in identifiable form	4,266	3,855	4,282
Number of systems requiring a Privacy Impact Assessment (PIA)	2,605	2,304	2,600
Number of systems with a PIA	2,319	2,135	2,414
Percentage of systems with a PIA	**89%**	**93%**	**93%**
Number of systems requiring a System of Records Notice (SORN)	3,373	2,997	3,366
Number of systems with a SORN	3,243	2,870	3,251
Percentage of systems with a SORN	**96%**	**96%**	**97%**

Privacy Program Oversight

In FY 2011, 23 out of the 24 CFO Act agencies' SAOPs reported participation in all three privacy responsibility categories (including privacy compliance activities, assessments of information

technology, and evaluating legislative, regulatory, and other agency policy proposals for privacy). One agency reported SAOP participation in two out of the three categories. In addition, all 24 agencies reported having policies in place to ensure that all personnel with access to Federal data are familiar with information privacy requirements, and 23 of the 24 agencies reported having targeted, job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 100% of applicable systems to have publicly posted PIAs. In 2011, 93% of applicable systems across the 24 CFO Act agencies had current PIAs covering applicable systems, the same percentage as 2010. The number of systems requiring a PIA, however, increased significantly.

Written Policies for Privacy Impact Assessments

In 2011, 23 of 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;
- Monitoring the agency's systems and practices to determine when and how PIAs should be updated; and
- Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained.

One agency reported having written policy for six out of the seven topics.

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

- Determining circumstances where the agency's web-based activities warrant additional consideration of privacy implications; and
- Making appropriate updates and ensuring continued compliance with stated web privacy policies.

System of Records Notices

The Federal goal is for 100% of applicable information systems with Privacy Act records to have developed, published, and maintained SORNs. In 2011, 97% of information systems government-wide with Privacy Act records have published current SORNs. This reflects an increase both in compliance as well as in the number of applicable systems.

Agency Use of Web Management and Customization Technologies

In 2011, 21 of 24 agencies reported use of these technologies. Of those 21 agencies, 20 reported having procedures for annual review, continued justification and approval for, and public notice of their use of web management and customization technologies.

VII. Path Forward

The collective efforts of Federal departments and agencies in FY 2011, in conjunction with DHS Federal Network Security (FNS) and EOP components, such as OMB and NSS, resulted in significant progress across the Federal Government in implementing critical capabilities, essential for a robust defensive cybersecurity posture. In FY 2012 and beyond, we will continue to drive progress in implementing these critical capabilities. Our collective focus will include:

- Driving the continued prioritization of cybersecurity investments across the Government through governmental working groups
- Coordinating common goals across agencies to focus cybersecurity efforts on the most cost effective controls and solutions
- Continuing to drive security improvement outcomes through quantifiable security metrics using measurable, repeatable, and automatable security metrics and measurement capabilities
- Minimizing technical barriers through the development of more technical reference architectures, intergovernmental working groups to bring together programs developing similar security requirements and capabilities, and the establishment of additional capability-targeted Tiger Teams
- Improving cost-effectiveness through the additional strategic sourcing efforts of the Information Systems Security Line of Business (ISSLOB)
- Expanding the FISMA Capabilities Framework and associated metrics to holistically, dynamically, and effectively mitigate the ever-evolving spectrum of threats and threat vectors targeting our infrastructures
- Finding and correcting technical vulnerabilities across the Federal Enterprise via technical risk and vulnerability assessments (RVAs) conducted by DHS/FNS and mitigation of associated findings
- Continuing to drive other key security initiatives forward, such as:
    - Developing Reference Architectures that provide best practices to agencies and assist them in complying with relevant Federal policies
    - Providing Shared Service Centers to improve the quality and reduce the costs of completing certification and accreditation
    - Providing Blanket Purchase Agreements to agencies to provide quick access to products and services
    - Conducting Red Team Blue Team activities to assist agencies with identifying security risks and to provide them with sound security engineering and management practices
    - Collaborating with the CISO Advisory Councils and Inspectors General on ways to improve Federal cybersecurity
    - Participating in Tiger Teams to provide solutions on how to enhance the security of Federal networks and systems

DHS will continue to focus on the implementation of the Administration FISMA priorities of Trusted Internet Connections, HSPD-12 and Continuous Monitoring. HSPD-12 implementation focuses agencies to upgrade their physical and logical access control infrastructure to require HSPD-12 PIV credentials for access to IT systems and facilities. Agencies will also finish consolidating all of their external network connections, so that all external traffic is routed through a TIC and will be expected to start to implement TIC v2.0 capabilities. Agencies that are still struggling to consolidate their network traffic will be encouraged to consider working with managed services provided by NETWORX vendors. In addition, agencies will implement continuous monitoring of operational IT assets by leveraging the work of the CIO Council Information Security and Identity Management Committee/DHS Continuous Monitoring Working Group, the NIST Security Content Automation Protocols (SCAP), the DHS Continuous Asset Evaluation Situational Awareness and Risk Scoring (CAESARS) Reference Architecture, and Information System Security Line of Business Blanket Purchase Agreements (currently SAIR TIER I) available through GSA.

A. Prioritizing Cybersecurity Investments

DHS will continue to focus on outcome oriented measures that are quantitative, specific, and focused on reduction of risk in order to enhance cybersecurity program monitoring, management, and reporting under the Federal Information Security Management Act (FISMA). Implementation of continuous monitoring will assist agencies in gaining efficiencies and improved effectiveness in securing their infrastructures in alignment with current FISMA reporting requirements.

Strengthening Security Management through CyberStat Model

DHS will continue work with agencies to identify and correct weaknesses in their cybersecurity programs. The reviews provide the opportunity for Agencies to identify the cybersecurity capability areas where they may be facing implementation maturity roadblocks, (e.g. technology, organizational culture, internal process, or human capital/financial resource challenges). In addition, CyberStat Reviews highlight areas where Agencies are meeting and exceeding required standards.

DHS will work in collaboration with agency Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to carefully examine agency-specific cybersecurity program data. The intended outcome is a time sensitive, prioritized action plan for the agency, informed by current operational challenges and events, to improve overall agency performance.

The CyberStat reviews and CIO interviews present the opportunity to stress to agencies the Administration Priorities and the metrics emphasized by the Administration. These included the metrics constituting continuous monitoring, TIC compliance and traffic consolidation, and HSPD-12 implementation. The Administration FISMA priority data used in the CyberStat reviews data was shared with the President's Management Council (PMC) and the Secretaries of the Departments. The high visibility given to these priority capabilities will help ensure continued steady progress in their implementation.

DHS interviewed each Federal civilian agency CIO and CISO on their agency's security posture, with the exception of those agencies selected for a formal CyberStat Review. The FY 2011 CIO Interview goals included assisting in assessing 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 FY 2011 CIO Interviews enabled DHS to track trends in the agencies' strategies to keep close and more consistent track of security vulnerabilities and threats. As the interviews move forward, identification of these trends will aid DHS in taking actions to improve the overall security posture of the Federal Government.

DHS provides quarterly tracking metrics to the President's Management Council (PMC) on the Administration priority measures. The PMC provides the opportunity to engage the Deputy Secretaries of the CFO Act Agencies to have them assist in driving implementation progress towards key strategic enterprise cybersecurity capabilities.

B. Minimizing Technical Barriers

DHS/FNS develops Cybersecurity Reference Architectures for Federal civilian agencies that minimize vulnerabilities in critical technologies including:

Trusted Internet Connections - The overall purpose of the Trusted Internet Connection (TIC) Initiative, as outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet. The initiative will 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.

Wireless Local Area Networks (WLAN) - The overall purpose of this Wireless Local Area Network (WLAN) Reference Architecture document is to provide Federal agencies a baseline to securely and efficiently implement a wireless architecture.

Domain Name System (DNS) Infrastructure - The overall purpose of the DNS Security Reference Architecture is to optimize and standardize the DNS currently in use by the Federal civilian government, and to improve the Federal Government's security posture by reducing the threats against the DNS at Federal civilian agencies.

Email Gateway Security - The purpose of the Mail Gateway Reference Architecture is to improve and standardize the Electronic Mail Gateways currently in use by the Federal Civilian Government, help departments/agencies (D/As) comply with FISMA mail security requirements and to improve the Federal Government's overall security posture by reducing electronic mail vulnerabilities.

Telework - The main objective of this document is to help agencies to securely implement a Telework infrastructure and ensure that those infrastructures comply with Federal cybersecurity requirements. This document presents a framework for planning, procuring, deploying, and maintaining Telework infrastructures with a focus on cybersecurity.

In FY 2012, DHS/FNS will continue to assist Federal departments and agencies to address technical barriers to implementing critical capabilities by developing reference architectures for mobile computing and data protection. Additionally, the DNSSEC Tiger Team will continue to support adoption of the National Strategy for Trusted Identities in Cyberspace (NSTIC) along with sponsoring technical training for DNSSEC and Email validation to be captured within the virtual training environment. New tiger teams will be created to address implementation issues for the most challenging critical capabilities.

C. Improving Cost-Effectiveness through Strategic Sourcing

In addition to studying agency security spending and architecture, 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 2011, ISSLOB established an updated set of requirements for Risk Management Framework services, based upon the updated NIST SP 800-37 Revision 1 and, leveraging the GSA Smartbuy Program, awarded 14 Blanket Purchase Agreements (BPAs) to private sector vendors to provide Risk Management Framework (formerly referred to as Certification and Accreditation)capabilities to Federal departments and agencies. Also in FY 2011, ISSLOB continued promoting the use of the Situational Awareness Incident Response (SAIR) TIER I BPA. Federal agencies purchasing products off the SAIR TIER I BPA have realized over $78 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 $11 million in cost avoidance and Certification & Accreditation – excluding DOI/NBC. BPD, and DOJ - showed more than $6 million in cost avoidance when compared to GSA Schedule 70 pricing.

ISSLOB has partnered with GSA SmartBUY and DoD on the SAIR TIER II solicitation and developed the requirements for SAIR III, Continuous Monitoring Tools, and will continue to work with its acquisition and Federal civilian agency partners to award the next round of BPAs in FY 2012 to continue delivering an economical means to implement security capabilities across the Federal enterprise. In FY 2012 the ISSLOB will be finalizing the Continuous Monitoring Tools requirements and exploring alternative methods to deliver the capabilities such as Conitnuous Monitoring as a Service, Qualified Products List and government wide purchases.

D. Expanding the FISMA Capabilities Framework

DHS will continue to focus FISMA on outcome oriented measures that are quantitative, specific, and focused on reduction of risk in order to enhance cybersecurity program monitoring, management, and reporting under FISMA. Incident and forensics data will be used to ensure that FISMA promotes the implementation of capabilities that most effectively mitigate the current threat. Continuous monitoring will be expanded to include threat monitoring and awareness of operational effectiveness. Departments and agencies will implement continuous monitoring to areas that have a significant threat presence and have been identified as the most critical for the protection of information resources. Insider Threat metrics will be added throughout the corresponding capabilities. Research indicates that the implementation of information security best practice and continuous monitoring can reduce insider threat incidents through a layered defense to include policy and procedures, as well as, information technology.

E. Finding and Correcting Technical Vulnerabilities across the Federal Enterprise

An increased emphasis will be placed on cybersecurity preparation and incident prevention through the execution of independent and objective cyber monitoring and risk assessment by DHS/FNS that will quantitatively measure, monitor, and validate implementation of cross-government cybersecurity initiatives and identify cyber risks on a recurring basis throughout the year.

DHS/FNS will focus on increasing the general health and wellness of the cyber perimeter. Activities will focus on broadly assessing all Internet accessible systems across the Federal Civilian Executive Branch for known vulnerabilities and configuration errors on a frequently recurring basis. As potential issues are identified, DHS will work with impacted agencies to proactively mitigate threats and risks to Federal systems prior to their exploitation by malicious third parties.

FNS will also target the CFO Act 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). Assessment teams will work with an agency to collaboratively analyze and independently test their systems for vulnerabilities using tools and tactics comparable to those of a malicious third party. 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 that will 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 the result will be an improvement in the cybersecurity preparedness of the Federal government and a reduction to the risk of malicious compromise of Federal systems and data.

F. Driving Key Security Initiatives Forward

The Administration is working aggressively to ensure that we can bring new technologies into the government more rapidly and more securely. Building on the progress of the last two-and-a-half years, the focus going forward will be to drive innovation in government and make investments in technology that better serve the American people. For example. through the "Shared First" initiative, we are looking for opportunities to shift to commodity IT, leverage technology, procurement, and best practices across the whole of government, and build on existing investments rather than re-inventing the wheel**.** We will use technology to improve government productivity and lower barriers to citizen and business interaction with the government, all while bolstering cyber security.

Empowering a Mobile Workforce with Wireless Security

The Administration is harnessing the transformative power of mobile computing and wireless platforms, applications and tools to provide the American people and Federal employees access to government information, services and resources when, where and how they want them. In order to seamlessly integrate mobile computing into government operations, we must minimize the inherent security risks associated with the technology.

In FY 2012, the Federal Government established a mobile government strategy task force (mGov Task Force), comprised of cross-agency representatives, to develop a strategy for accelerating the adoption of mobile/wireless technologies in the Federal sector. The Federal Mobility Strategy, slated to be released in March 2012, will include mGov Task Force recommendations for addressing the security and privacy implications of Federal mobility. OMB will also establish a formal mobility governance structure that will manage the development and updating of policies, procedures and standards that allow for the safe and expeditious adoption of mobile technology.

In addition, NIST will issue a public draft guideline for *Managing and Securing Mobile Devices in the Enterprise* and a NIST Interagency Report (NISTIR) for *Testing Third Party Developed Mobile Apps*. The special publication introduces recommendations for organizations to centrally manage and secure mobile devices throughout their lifecycle and provide mitigation techniques against known threats such as information leakage and disclosure, malicious content, lost devices, insecure protocols, and untrusted apps. The objective of the NISTIR is to provide a methodology for testing and vetting third-party developed applications that are distributed through various app stores.

Supporting Telework

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. It is expected that FY 2012 will see growth in Federal Government teleworking given advancements in implementing the Telework Enhancement Act of 2010 and other telework initiatives.

If telework is not properly implemented, it may introduce new information security and privacy vulnerabilities into agency systems and networks. To address these concerns, in 2011, OMB issued M-11-27 reiterating that agencies must adhere to the requirements of FISMA. Following the release of this OMB memorandum, DHS/FNS issued the "Telework Reference Architecture" document. This document outlines how Federal agencies should securely implement a telework infrastructure and presents a framework for planning, procuring, deploying, and maintaining telework infrastructures with a focus on cybersecurity to prevent vulnerabilities into agency systems and networks. Additionally, to better understand and manage these vulnerabilities, telework performance metrics through CyberScope will continue to be collected. As the number of Federal employees' teleworking grows in FY 2012 and beyond, these metrics will be examined closely and revised to address the information security and privacy risks brought by the increasingly dispersed Federal workforce.

Ensuring a Safe and Secure Adoption of Cloud Computing

The Federal government's current Information Technology (IT) environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times. As part of a comprehensive effort to increase the operational efficiency of Federal technology assets and deliver greater value to the American taxpayer, the Federal government is rapidly shifting to the deployment of cloud services. The emergence of cloud computing provides a once in a generational opportunity to close the IT productivity gap between the public and private sectors. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints, to do more with less.

In order 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 IT Management[18]. The Administration also published the Federal Cloud Computing Strategy[19], which articulates the benefits, considerations, and trade-offs of cloud computing, provides a decision framework and case examples to support agencies in migrating towards cloud computing, highlights cloud computing implementation resources, and identifies Federal Government activities, roles, and responsibilities for catalyzing cloud adoption. Furthermore, a "cloud first" policy[20] was established. Under this policy, agencies are required to evaluate safe, secure cloud computing options before making any new investments. If such an option exists, then agencies must use the cloud solution as the default. This policy will fundamentally change the way the Federal government buys IT by shifting from an asset mindset to one of service delivery. The new policy has already produced

---

[18] 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

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

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

results. In 2011, under the IT Reform Plan, Federal agencies migrated 40 services to cloud computing environments, with an additional 39 services to be migrated in 2012.

It was also noted in our Federal Cloud Computing Strategy, that the government would continue to address the challenges posed by cloud computing. These challenges have been noted by stakeholders within agencies, Congress and industry. The most notable of these challenges and the one most often cited as the largest barrier to cloud adoption is security. As more Federal systems and users move to cloud computing environments, the government must ensure the safety, security and reliability of its data. Just as our broader cybersecurity efforts have shifted to a real time, continuous posture from a paper based one, our efforts on security and cloud computing will evolve over time.

The next step in this evolution is the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP will change the way the Federal government secures cloud solutions by providing a uniform risk management approach that uses a standard set of baseline security controls that will be used government-wide. The Program allows joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use. Continuous monitoring coordination is essential to provide agencies the ability to facilitate their risk management processes by reporting the security posture of their IT assets residing in the cloud. Joint authorization of cloud providers results in a common security risk model that can be leveraged across the Federal government. The risk model will also enable the government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's authorization and access to service providers' authorization packages. Currently, the Federal government spends hundreds of millions of dollars a year securing the use of IT systems in a duplicative, inconsistent, and time consuming manner. We expect FEDRAMP to result in significant cost savings when assessing, authorizing, and continuously monitoring cloud solutions.

In support of the Federal cloud computing efforts, NIST is developing a Federal government cloud computing roadmap. The purpose of the roadmap is to foster Federal agencies' adoption of cloud computing, support the private sector, improve the information available to decision makers and facilitate the continued development of the cloud computing model.

Additionally, NIST is collaborating with a broad group of stakeholders to reach consensus on cloud security, portability and interoperability standardization priorities while GSA is working to develop and make available to agencies secure government-wide cloud procurement vehicles. 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.

Standardizing Security through Configuration Settings

Secure configuration settings allow agencies to reduce risks across their enterprise by deploying settings that are more secure than the default manufacturer settings out of the box. When properly implemented, they reduce risk by mitigating vulnerabilities and limiting exposure to threats. When

deployed standard configuration settings enable agencies to more effectively monitor and maintain their systems.

In FY 2010, DOD, DHS, NIST and the Federal CIO Council worked closely together to develop the United States Government Configuration Baseline (USGCB) for Windows 7 and Internet Explorer 8. As a baseline, USGCB is the core set of default security configurations for all agencies; however agencies may make risk-based decisions and customize the USGBC baseline to fit their operational needs.

This year the USGCB for RedHat Enterprise Linux 5 Desktop was developed and multiple updates for Windows 7 and Internet Explorer 8 were implemented. NIST also updated the SCAP Validation Program to include USGCB test requirements and test tools. Accredited laboratories are now able to validate product capability to process USGCB SCAP content and produce SCAP compliant results.

In FY 2012 USGCB settings will be updated and maintained to account for challenges or upgrades and the USGCB will incorporate additional products to allow for increased deployment of secure settings across the Federal Government.

Preventing the Purchase of Counterfeit Products

The prevalence of counterfeit goods in the U.S. Government supply chain is concerning. Reports issued by the Department of Commerce and the Government Accountability Office have found that counterfeit goods have infiltrated many sectors of the U.S. Government supply chain for a wide range of products from electronic components to brake pads to bullet proof vests. These counterfeits pose threats to public health and safety, national security, and the successful accomplishment of key Government objectives. The Administration's 2010 Joint Strategic Plan on Intellectual Property Enforcement recognized this threat and took concrete steps to address it by establishing a government-wide working group to prevent the purchase and use of counterfeit products.

Over the last year, the Intellectual Property Enforcement Coordinator (IPEC) convened and chairs the group made up of subject matter experts from 14 government agencies that are responsible for identifying gaps in legal authority, regulation, policy and guidance that preclude an optimal Federal Government procurement approach, compare progress, and share best practices to ultimately eliminate counterfeits in their supply chains. The Office of Federal Procurement Policy (OFPP), Departments of Defense and Justice, and the National Aeronautical and Space Administration (NASA) have assumed leadership roles within the working group based on their vast expertise with U.S. Government procurement and anti-counterfeiting practices.

The group's objectives include the review of risk assessment by agency program managers, supplier requirements to address counterfeiting, traceability to confirm production authority by the original manufacturer of at-risk items, testing and evaluation, training and outreach, and enforcement and remedies. The working group has conducted outreach both within government and with external stakeholders to inform its efforts. A report setting out the Administration's strategy and specific

steps the agencies will take to reduce the risk of counterfeits in the U.S. Government supply chain will be released in 2012.

G. Preventing Unauthorized Disclosure

Just over one year ago, the Wikileaks incident served as a strong reminder to the government that preventing the unauthorized disclosure of classified and sensitive government information must be an ongoing priority for every Federal Agency. In September, the Administration completed a thorough review of the incident that included Agency assessments of their ability to protect classified and sensitive information from insider threats and external attacks. As a result, on October 7th, 2011 the President issued Executive Order 13587 on Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. This Order established a Senior Executive Steering Committee co-chaired by the National Security Staff and the Office of Management and Budget to oversee the development of policy and standards regarding classified information sharing and safeguarding. The Order also directed the establishment of an Insider Threat Task Force (ITTF) to develop an insider threat program to deter, detect, and mitigate insider threats Government-wide. The ITTF program is designed to safeguard classified and sensitive information from exploit, compromise, and unauthorized disclosure through the following objectives:

- Establish the U.S. Government policy by which heads of Executive Branch departments and agencies shall develop, implement and maintain an insider threat program to deter, detect, and mitigate against compromise, unauthorized use or unauthorized disclosure of sensitive information; one that integrates 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.
- Provide a governance structure for protection against those insiders who would use their authorized access to do the government harm wittingly or unwittingly.
- Strengthen the U.S. Government safeguarding postures through viable and effective Insider Threat Detection programs to enhance the protection of National Security Information.
- Strengthen the U.S. Government safeguarding postures by establishing policy and standards for a National Insider Threat detection and prevention program that will enhance the protection of national security information.
- Assist departments and agencies to establish viable Insider threat detection and prevention programs through periodic consultations and assistance visits.
- Develop assessment procedures and, as directed by the Steering Committee, conduct on-site evaluations to determine the adequacy of department and agency Insider Threat programs to meet related policy and standards.

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.

Appendix 1: Inspectors General's Findings

Each inspector general (IG) was asked to assess his or her agency's information security programs in the following eleven areas:

- Risk management
- Configuration management
- Incident response and reporting
- Security training
- Plans of actions and milestones (POA&M)
- Remote access management
- Identity and access management
- Continuous monitoring management
- Contingency planning
- Contractor systems
- Security capital planning[21]

IGs were asked to evaluate 127 attributes in each of these eleven areas and determine whether: (1) that the agency had established and maintained a program that was generally consistent with NIST and OMB's FISMA requirements, and included the needed attributes; (2) the agency had established and maintained a program that needed significant improvements; or (3) the agency had not established a program for the area. If an agency's program for a certain security area needed improvements, the IG identified the issues and required improvements from a list of possible problem issues for each of the eleven areas. If an issue and the needed improvement did not appear on the area's list of issues, the IG provided a narrative describing the issue and the needed improvements. IGs could report that a program was generally consistent with requirements, but still mark specific attributes as non-compliant. This possibility was not available in FY 2010 reporting requirements and resulted in a minor modification to 2011's scoring formula.

Table A summarizes the results from the IGs of the 24 CFO Act agencies according to cyber security program area. These results indicate that the agencies 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.

[21] Security capital planning was a new metric for FY 2011

Table A: Results for CFO Act Agencies, by Cyber Security Area

Cyber Security Program Area	Compliant Program			Needs Improvement			Program Not Implemented		
	FY11	%	FY10	FY11	%	FY10	FY11	%	FY10
Risk Management	8	33	13	16	67	11	0	0	0
Configuration Management	6	25	6	18	75	18	0	0	0
Incident Response and Reporting	16	67	15	8	33	9	0	0	0
Security Training	12	50	7	12	50	17	0	0	0
POA&M	6	25	8	18	75	16	0	0	0
Remote Access Management	13	54	10	11	46	14	0	0	0
Identity and Access Management	6	25	5	18	75	19	0	0	0
Continuous Monitoring Management	9	37	7	12	50	15	3	13	2
Contingency Planning	8	33	8	16	67	16	0	0	0
Contractor Systems	10	42	6	14	58	16	0	0	2
Security Capital Planning	16	67	N/A	8	33	N/A	0	0	N/A

Table B provides CFO Act agencies compliance scores. The Department of Defense did not provide sufficient information for scoring. The Nuclear Regulatory Commission, National Science Foundation, and Social Security Administration had compliant programs in place for all eleven areas, although each did identify areas for improvement. The remaining agencies had at least one area that needed significant improvement. Three agencies—the Department of Housing and Urban Development, Office of Personnel Management, and the Agency for International Development—all reported that they did not have continuous monitoring management programs in place. In FY 2010, all three of these agencies reported having a continuous monitoring program at least partially in place, while two different agencies reported not having a continuous monitoring program —an indication of gains in some areas and losses in others. Total numbers of areas with deficiencies were used to compute compliance scores. Seven agencies scored over 90 percent compliance, eight scored between 65 and 90 percent compliance, and the remaining eight scored less than 65 percent. The average score across the agencies was 72.8 percent. Nine agencies improved over their FY 2010 scores, with NASA showing the largest gain of 32.1 points. Eleven agencies had scores that were lower that their FY 2010 scores. The United States Agency for International Development had the largest decline of 36.6 points. Three agencies maintained their scores from 2010 within +/- 1 point.

Table B. CFO Act Agencies' Compliance Scores, Based on IGs' Reviews

Agency	FY11 (%)	FY10 (%)	Change
National Science Foundation	98.8	98.9	-(0.1)
Social Security Administration	96.9	100	-(3.1)
Environmental Protection Agency	94.9	99.2	-(4.3)
Nuclear Regulatory Commission	94.8	96.7	-(1.9)
Department of Homeland Security	93.4	92.5	0.9
National Aeronautics and Space Administration	92.9	60.8	32.1
Department of Justice	91.2	85.8	5.4
Department of Energy	84.3	84.6	-(0.3)
General Services Administration	84.2	87.6	-(3.4)
Department of Commerce	81.4	77.9	3.5
Department of the Treasury	79.4	86.4	(-7.0)
Office of Personnel Management	78.6	57.8	20.8
Department of Labor	71.6	44.5	27.1
Small Business Administration	68.7	50.3	18.4
Department of Housing and Urban Development	66.1	87.3	-(21.2)
Department of State	63.2	79.4	-(15.2)
Department of Education	57.5	71.9	-(14.4)
United States Agency for International Development	53.8	90.4	-(36.6)
Department of Veterans Affairs	52.8	57.0	-(4.2)
Department of Health and Human Services	50.9	64.7	-(13.8)
Department of Transportation	44.2	29.8	14.4
Department of the Interior	42.2	24.6	17.6
Department of Agriculture	32.5	13.7	18.8
Department of Defense	N/A	N/A	N/A*

*DOD did not provide the answers with the detail required for scoring in FY10 or FY11

The Eleven Cyber Security Areas

Risk Management. The risk management framework is a key component of Federal information security. Every information technology system presents risks, and security managers must identify, assess, and mitigate systems' risks. Agency executives rely on accurate and continuous assessment of a system, since they are ultimately responsible for any risks posed by the system's operation.

Compliance with risk management requirements suffered the largest decline of any metric between FY 2010 and 2011. IGs for 8 of the 22 agencies reported that their agencies had compliant programs, while 13 of 24 IGs reported full compliance in 2010. The remaining 16 agencies, however, had programs in place that need improvements. The following deficiencies were the most common[22]:

- Accreditation boundaries for agency systems were not defined (13 of 23 agencies);
- Insufficient communication of specific risks to appropriate levels of the organization (12 of 23 agencies);
- Risks from a mission or business process perspective are not addressed (12 of 23 agencies);
- Security control baselines were not appropriately tailored to the individual systems (11 of 23 agencies);
- Security assessment report is not in accordance with government policies (11 of 23 agencies).

Configuration management. In order to secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. OMB requires all Windows XP, Vista, and 7 work stations 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, configuration management is one of the areas that need the most improvement. While all agencies had configuration management programs, 18 of 24 agencies' programs needed significant improvements. The following deficiencies were the most common:

- Configuration management policy is not fully developed (13 of 23 agencies);
- Configuration management procedures are not fully developed (9 of 23 agencies);
- Standard baseline configurations are not identified for all hardware components (9 of 23 agencies);
- FDCC/USGCB is not fully implemented (8 of 23 agencies).

Incident response and reporting. Information security incidents occur on a daily basis, and agencies must have sound policies and planning in place to respond to incidents and report them to

[22] For the detailed listing of common deficiencies, only 23 agencies are considered, as DoD did not provide answers by metric.

the appropriate authorities. OMB has designated the 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. Sixteen IGs reported that their agencies had incident response and reporting programs in place and that the programs were fully compliant with applicable standards, which was the same total as FY 2010. The remaining eight IGs identified areas in need of significant improvement. The following deficiencies were the most common:

- Incident response and reporting policy is not fully developed (8 of 23 agencies);
- Incidents were not reported to law enforcement as required (7 of 23 agencies);
- The agency does not have the technical capability to correlate incident events (6 of 23 agencies).

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, agencies cannot provide appropriate training or ensure that all personnel receive the required training.

Security training was the most improved metric. Twelve of the 24 IGs reported that their agencies were fully compliant, while in FY 2010, only 7 had compliant programs. However, twelve IGs reported that significant improvements were needed to make their agencies fully compliant with applicable requirements. The following deficiencies were the most common:

- Security awareness training policy is not fully developed (11 of 23 agencies);
- Training material for security awareness training does not contain appropriate content for the Agency (11 of 23 agencies);
- Specialized security training procedures were not fully developed or sufficiently detailed (9 of 23 agencies).

Plans of Action and Milestones (POA&M). When weaknesses in information security systems are identified as the result of controls testing, audits, incidents, continuous monitoring, or other means, they must be recorded within a POA&M. This plan provides security managers, accreditation officials, and senior officials with a view of the weakness's overall risk to the system, planned actions to address the risk, associated costs, and expected completion dates.

All 24 IGs indicated that their agencies had POA&Ms in place. However, 18 IGs also indicated that their agency programs needed significant improvements, two more than FY 2010. Ten or more IGs identified the following seven problems:

- POA&M Policy is not fully developed (14 of 23 agencies);

- Security weaknesses are not appropriately prioritized (14 of 23 agencies);
- Source of security weaknesses are not tracked (13 of 23 agencies);
- Agency CIO does not track and review POA&Ms (12 of 23 agencies);
- POA&Ms are not updated in a timely manner (11 of 23 agencies);
- POA&M procedures are not fully developed and sufficiently detailed (10 of 23 agencies);
- Remediation actions do not sufficiently address weaknesses in accordance with government policies (10 of 23 agencies).

Remote access. Secure remote access is essential to agency operations because the proliferation system access through telework, mobile devices, and information sharing has made information security no longer confined to system perimeters. Agencies 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.

While no agency reviewed lacked a remote access program, 13 of 24 IGs reported that agencies had compliant programs in place, 3 more than in FY 2010. The remaining 11 IGs indicated that their agencies needed to implement significant improvements to fully comply with security requirements for remote access. The most common remote access weaknesses were:

- Lost or stolen devices are not disabled and appropriately reported (10 of 23 agencies);
- Remote access policy is not fully developed (8 of 23 agencies);
- Agency cannot identify all users who require remote access (8 of 23 agencies).

Identity and access management. Proper identity and access management management ensure that users and devices are properly authorized to access information or 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, while 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. The use of Personal Identity Verification (PIV) cards by all agencies required by Homeland Security Presidential Directive 12 is a major component of a secure, Government-wide account and identity management system.

Identity and access management was identified as an area most in need of improvement. Only 6 of the 24 IGs reported that their agencies had fully compliant programs in place, 1 more than in FY 2010. The remaining 18 IGs all identified areas of their agencies' account and identity management programs that needed significant improvements. The most common control weaknesses identified by the IGs were:

- The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies (15 of 23 agencies);
- Account management policy is not fully developed (14 of 23 agencies);

- Agency cannot identify all User and Non-User Accounts (13 of 23 agencies);
- Use of shared privileged accounts is not necessary or justified (13 of 23 agencies);
- When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group (13 of 23 agencies).

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.

Based on the IGs' reviews, agencies' continuous monitoring programs needed the most improvement. While the number of agencies with compliant programs increased from 7 in FY 2010 to 9, the number of agencies without any continuous monitoring management increased from 2 to 3. The other 12 agencies needed to implement significant improvements to make their programs fully compliant. The weaknesses in continuous monitoring management most reported by those ten IGs were:

- Continuous monitoring policy is not fully developed (9 of 23 agencies);
- Providing key security documentation to the system authorizing official or other key system officials (8 of 23 agencies);
- Continuous monitoring procedures are not consistently implemented (7 of 23 agencies).

Contingency planning. FISMA requires agencies to prepare for events that may affect the availability of an information resource. This preparation entails identification of important agency resources and potential risks to those resources, and development of a plan to address the consequences if those risks are realized. Consideration of the risk to an agency's mission and the potential magnitude of harm if a resource becomes unavailable are key to sufficient contingency planning. Critical systems may require multiple, 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. Contingency planning is essential for decision-making before a disaster actually occurs. Once a plan is in place, training and testing must be conducted to ensure that the plan will function in the event of an emergency.

All 24 IGs reported that their agencies had contingency planning programs in place, but as in FY 2010, only 8 IGs identified their agencies' contingency planning programs as fully compliant with standards. The following five issues were prevalent among the 16 agencies needing improvements:

- Alternate processing sites are subject to the same risks as primary sites (14 of 23 agencies);
- Backups are not properly secured and protected (13 of 23 agencies);
- Contingency planning policy is not fully developed contingency planning policy is not consistently implemented (12 of 23 agencies);
- Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (10 of 23 agencies);
- Backups of information are not performed in a timely manner (11 of 23 agencies).

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

Oversight of contractor systems improved significantly, with ten IGs now reporting their agency is fully compliant, compared to six in FY 2010. Furthermore, all IGs reported that their agencies had programs contractor oversight programs this year, while in FY 2010, two IGs reported that their agencies had no programs. Fourteen IGs indicated that their agencies' programs needed significant improvement. The most common weaknesses reported were:

- Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (12 of 23 agencies);
- Policies to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed (10 of 23 agencies);
- The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (9 of 23 agencies).

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

This metric, new in FY 2011, received the highest score, with 16 of 24 IGs reporting that their agencies were fully compliant. Eight IGs reported that their agencies' programs were in place, but needed significant improvements. The most common weaknesses reported were:

- The Agency does not provide IT security funding to maintain the security levels identified (6 of 23 agencies);
- CPIC information security policies and procedures are not fully developed (5 of 23 agencies).

Appendix 2: NIST Performance in 2011

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 2011, CSD addressed its assignments through the following projects and activities:

- Issued 17 final NIST Special Publications (SPs) that provided management, operational, and technical security guidance in areas such as: BIOS protection, cloud computing, configuration management, cryptography, industrial control system security, information security continuous monitoring, key management, security automation, and virtualization. In addition, 19 draft SPs on a variety of topics, including: cloud computing, cryptographic key management, electronic authentication, personal identity verification, and risk assessments, were issued for public comment;
- Continued the successful collaboration with the Office of the Director of National Intelligence, 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;
- Provided assistance to agencies and the private sector: conducted ongoing, substantial reimbursable and non-reimbursable assistance support, including many outreach efforts such as the Federal Information Systems Security Educators' Association (FISSEA), the Federal Computer Security Program Managers' Forum (FCSM Forum), and the Small Business Corner;
- Reviewed security policies and technologies from the private sector and national security systems for potential Federal agency use: hosted a growing 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 on draft standards and guidelines and on information security and privacy issues regularly at quarterly meetings;
- Provided outreach, workshops, and briefings: conducted ongoing awareness briefings and outreach to CSD's customer community and beyond to ensure comprehension of guidance and awareness of planned and future activities. CSD also held workshops to identify areas that the customer community wishes to be addressed, and to scope guidelines in a collaborative and open format; and
- Produced an annual report as a NIST Interagency Report (NISTIR). The 2003-2010 Annual Reports are available via our Computer Security Resource Center (CSRC) website.

Appendix 3: 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 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