Fiscal Year 2010
Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

Table of Contents

Figures

Tables

I. Introduction: Current State of Federal Information Security

The Federal government provides thousands of essential services, ranging from disaster assistance to social security to national defense. These services are dependent on a safe, secure, and resilient information technology (IT) infrastructure. Threats to this 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 Executive Branch 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 risk and magnitude of harm. This *Fiscal Year 2010 FISMA Report to Congress* provides the status of Federal-wide and Agency-specific information security initiatives and compliance with FISMA requirements.

Among other accomplishments, in Fiscal Year (FY) 2010 the Federal government:

- Shifted from periodic security reviews to continuously monitoring and remediating IT security vulnerabilities. The move towards continuous monitoring and automation has raised our awareness of our own networks and allowed us to collect the information we need to better secure government information systems.
- Developed new information security performance metrics and began regularly collecting data on those metrics across government to drive outcome-focused security management practices.
- Implemented the National Institute of Standards and Technology (NIST) "Risk Management Framework" concepts as part of continuous monitoring procedures, moving away from the Certification & Accreditation process.[2]
- Achieved new service and acquisition efficiencies through strategic sourcing of security products.
- Approved the National Initiative for Cyber Education (NICE) to improve cybersecurity education through the establishment of operational, sustainable education and training programs for multiple groups, including academic and professional development.

Moving forward, these approaches have established a foundation upon which a new structure of Federal information security is being built: informed by the minute-by-minute reality of our networks, responsive to ever-changing threats, and readily managed by Federal agencies large and small.

This foundation will allow for a better partnership with industry to continually bring the best information security techniques and technology to Federal agencies. It will bring increased

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

[2] NIST Special Publication 800-39: *Integrated Enterprise-Wide Risk Management Organization, Mission, and Information System View*. December, 2010.

information sharing between industry and government to share best practices and information on emerging threats and vulnerabilities. Most importantly it will reduce the barriers that exist to bring new technology into the Federal government and allow for agencies to better fulfill their missions and meet the needs of the American public.

The following sections of the *Fiscal Year 2010 FISMA Report to Congress* identify major areas of progress, present key analyses, and discuss future directions and actions for advancing the implementation of FISMA and continuing the improvement of information security in the Federal government. This report also highlights how various information security guidelines developed by NIST are being implemented by the Federal government and how such implementations contribute to security improvements. A summary of NIST activities and performance in FY 2010 on information security is provided in Appendix 2.

II. FY 2010 Progress: A Focus on Execution

When FISMA was initially enacted, the government had little or no insight into the security of its information infrastructure. At first, the mandate of FISMA was largely met by requiring Certification and Accreditation (C&A), a process which led to detailed audits and inventories of Federal Agency information systems. While this approach provided foundational work to understand where information and information systems assets were found across the government and provided a baseline of security controls for those assets, it did not recognize or respond to the real-time nature of the threats to Federal information systems.

In many agencies, large aspects of FISMA implementation became an additional compliance exercise, related to, but removed from, their information security mission. Data that could be analyzed by security professionals to better protect agency systems would not be available until well after it could serve this purpose. It became clear that compliance alone would never get the Federal government to the right level of information security.

As a result, many agencies began to develop new methods to protect their systems that often went well beyond what was required by policy or regulation. In the past few years, the Federal government as a whole has begun to harness these techniques developed by forward-thinking agencies – as well as industry best practices – to move FISMA implementation toward the real-time detection and mitigation of security vulnerabilities.

Critical to this new approach is the interagency policy process led by the White House Cybersecurity Coordinator and the implementation leadership of the Department of Homeland Security (DHS) in its role as a robust operation center for Federal information security.[3] Through

[3] OMB M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*. This memorandum clarified that DHS has primary responsibility for the operational aspects of Federal Agency cybersecurity.

the Trusted Internet Connection[4] and Einstein[5] initiatives, DHS has had growing insight into the threats to, and the vulnerabilities of, information systems across government and has developed a core situational awareness.

In FY 2010, agencies started reporting detailed security metrics through Cyberscope, a Federal system to capture operational pictures and to gain insight into agency information security practices. Armed with more insight into agency-level security posture, DHS hosted individual meetings with agencies to discuss the new approach, request additional information, and establish meaningful dialogue with agencies' senior leadership and key information security personnel.

The next step in this evolution in FY 2011 will be the introduction of the "CyberStat" management model throughout the Federal government. These meetings will bring agency leadership together to examine the metrics reported through Cyberscope and develop in-depth remediation plans to quickly address any issue. Through CyberStats, DHS will also be able to evolve security metrics and assist agencies to enhance data quality and completeness. Combining CyberScope and CyberStat together, this approach gives agencies information they have never had before about risks to their information and information systems; it also allows DHS to examine and correlate the data on risks across the entire federal enterprise and to provide such knowledge back to agencies.

A. Continuous Monitoring and Remediation

A key element to managing an information security program is having accurate information about security postures, activities and threats. Conducting a thorough point-in-time assessment of the deployed security controls is a necessary, but not sufficient, step to demonstrate security due diligence. Agencies need to be able to monitor security-related information from across the enterprise in a manageable and actionable way. The many levels of agency management all need different levels of this information presented to them in ways that enable effective decision making.

A well-designed and well-managed continuous monitoring[6] 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-related information to

[4] The Trusted Internet Connections (TIC) initiative was announced in OMB memorandum M-08-05. TIC targets at optimizing Federal government's individual network services into a common solution for the Federal government. This common solution facilitates the reduction of Federal government's external connections, including its Internet points of presence, to a target of fifty.

[5] The Einstein initiative established a government-wide intrusion detection system that monitors the network gateways of Federal government agencies for unauthorized traffic. The software was developed and is being operated by the United States Computer Emergency Readiness Team (US-CERT).

[6] According to the Draft NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

organizational officials. This in turn allows appropriate risk mitigation actions and cost-effective, risk-based decisions regarding the operation of the information system. While these programs benefit from the latest technology, this approach is at its core about effective management – allowing for decisions to be made quickly, based on timely and accurate information.

During FY 2010, agencies continued the shift to continuous monitoring, building upon the foundational efforts in FY 2009, which included the development of the Cyberscope platform to streamline agency reporting and the implementation of security metrics to advance insight into agency security postures.

Cyberscope, launched in FY 2010, is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a Federal agency's information infrastructure. The broad range of metrics collected, the use of secure two-factor authentication using Personal Identity Verification (PIV) cards, and the online access to data provide for a more efficient and effective reporting process and enable a focus on more meaningful analyses of security postures.

In April 2010, the Office of Management and Budget (OMB) directed all agencies to adopt a three-tiered approach for security reporting through Cyberscope.[7] This approach is the result of a task force established in September 2009 to develop new, outcome-focused metrics for information security performance for Federal agencies.[8] The approach included the following elements:

- **Data feeds directly from security management tools –** In the fourth quarter of FY 2010, some agencies began reporting on information collected from agency security monitoring systems in the following areas:
  - Inventory
  - Systems and Services
  - Hardware
  - Software
  - External Connections
  - Security Training
  - Identity and Access Management
- **Government-wide benchmarking on security posture –** A set of questions on the security posture of the agencies was included in Cyberscope.
- **Agency-specific interviews –** As a follow-up to the questions described above, a team of government security experts interviewed agency Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) individually on their respective security

[7] OMB Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. April 21, 2010.

[8] Participants in the Security Metrics Task Force included the Federal CIO Council, the Department of Defense, and the Office of the Director of National Intelligence; the Council of Inspectors General on Integrity and Efficiency; and the Information Security and Privacy Advisory Board. In addition, the Government Accountability Office (GAO) served as an observer to this taskforce.

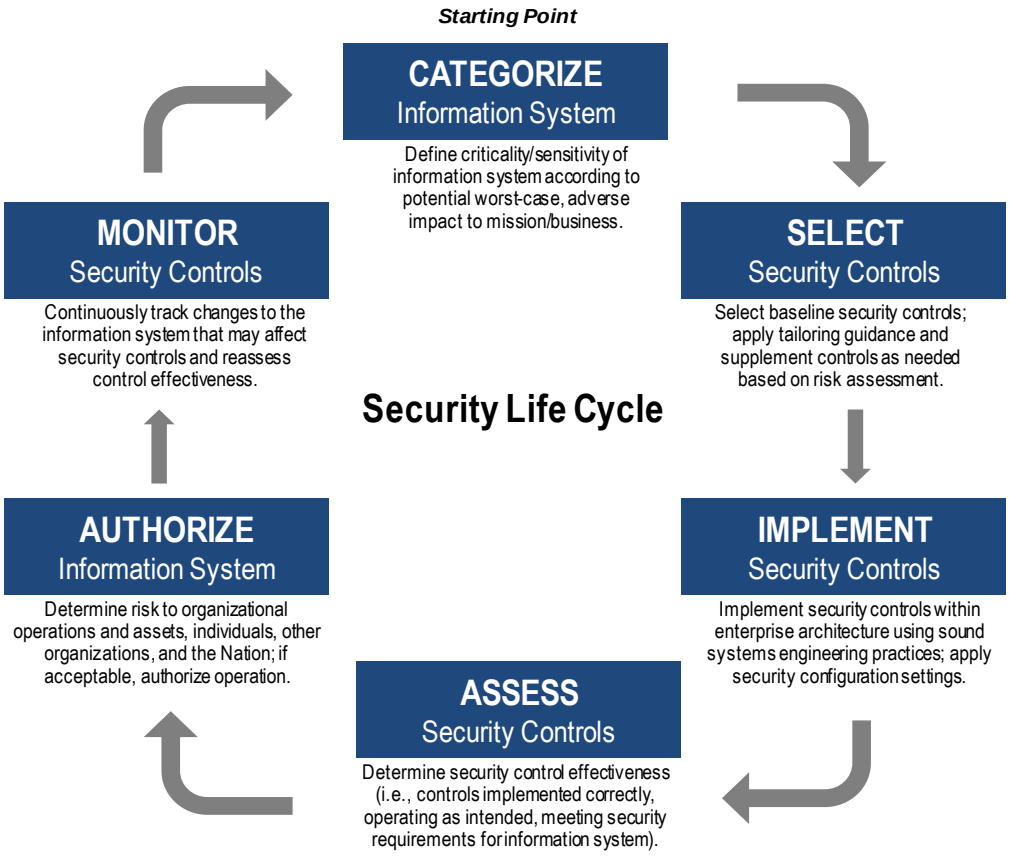
postures. The interviews, conducted by the DHS' Federal Network Security (FNS) Branch, were designed to assist in assessing each agency's FISMA compliance and challenges and to identify security best practices. Additionally, the process served to raise awareness of FISMA reporting requirements, and establish meaningful dialogue with agencies' senior leadership.

- **Red/Blue Teams –** In 2010, DHS initiated the development of a new portfolio of Red/Blue team services[9] to be offered to support Federal Civilian Executive Branch agencies through one-on-one engagements that will provide agencies with objective information and expert services necessary to identify and mitigate their distinct cyber risk. DHS met with several (Red/Blue) security teams throughout the Federal government to understand the services they provide, the process and procedures necessary to execute those services, and to capture practical advice and lessons learned. DHS subsequently issued a Concept of Operations Document and will be building out the Red/Blue team services going forward.
- **Risk Management Framework –** In February 2010, NIST published Special Publication (SP) 800-37 Revision 1; *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*. This publication transformed the traditional information system C&A process into a six-step Risk Management Framework[10] (Figure 1).

[9] Blue teams are comprised of security professionals and provide services designed to assess and validate the security of information technology systems. The red team works independently to test systems for vulnerabilities using tools and tactics comparable to those of an attacker while the blue team works in coordination with the agency to assess and validate the technical capabilities (tools and technologies) and operational readiness (people, processes, security program maturity); the goal is both to validate compliance with national cybersecurity initiatives, policies and standards and to objectively quantify risks and identify vulnerabilities so agencies can implement the necessary corrective actions to better protect their systems.

[10] Chapter Three of NIST 800-37 R1 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



This Risk Management Framework provides the foundation for assuring information security capabilities within Federal information systems through the application of specific managerial, operational, and technical security controls; maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring; and providing essential information to senior leaders. This framework facilitates decisions regarding the acceptance of risk related to the operation and use of information systems.

B. Information Security Workforce

A skilled and trained workforce, well-prepared to secure cyberspace, is essential to effective Federal information security. Significant amounts of security automation have begun to enable agencies to scale and gain visibility into vast and complex infrastructures; however, the demand for personnel, with ever more sophisticated skills, will continue to climb as we focus upon these increasingly technical aspects of the information security mission.

Federal agencies are working aggressively to increase the professionalization of the cybersecurity workforce.[11] The Office of Personnel Management (OPM) is developing a

[11] The National Initiative for Cybersecurity Education (NICE), led by the NIST, has evolved from the Comprehensive National Cybersecurity Initiative (CNCI), and contains two tracks specifically focusing on the Federal workforce. The Office of Personnel Management (OPM) is

cybersecurity competency model and reviewing human resource strategies to help hire and retain cybersecurity experts to meet existing and future Federal workforce needs. The Federal CIO Council's IT Workforce and Information Security and Identity Management Committees are conducting research on the information security environment to develop role-based information security workforce development matrices. The matrices are intended to establish a baseline across the Federal government for staff engaged in information security work and identify a common framework describing competencies/skills, education, experience, credentials and training needed by performance level for critical information security roles.

C. Information Security Performance Metrics

In previous years, FISMA's implementation included the collection of metrics that represented a number or percentage of systems and organizations that were in compliance with security standards. In 2009, the Security Metrics Task Force[12] defined new FISMA performance and outcome-based metrics. These information security performance metrics highlight risk and areas needing improvement for Federal agencies. Most importantly, the metrics are designed to assess the implementation of security capabilities, measure their effectiveness, and ascertain their impact on risk levels.

To support FISMA reporting in 2010, Federal agencies began tracking these new metrics to determine a Government-wide baseline on the security posture of the Federal enterprise. In addition to supplying an overall view of security across the Federal enterprise, the metrics empower individual agencies with the knowledge and understanding of how best to address their particular areas of weakness. Agencies can use a risk management process to determine how to prioritize resources and funding to obtain the largest improvement in security and the greatest return on investment.

In FY 2010, the Federal government established the new reporting foundation and tracked three categories of metrics:

- Implementation level metrics (i.e. does the capability implemented allow the capture of the outcome-oriented data?)
- Effectiveness metrics (i.e. was the capability implemented properly?) and when these metrics show progress
- Outcome/impact metrics (i.e. how many and which vulnerabilities exist in our infrastructure?)

Going forward, the metrics will be refined to provide a more in-depth view of the implementation and effectiveness of security controls. As continuous monitoring and its supporting technologies become more mature and widely implemented, the metrics will collect

---

responsible for the Federal Cybersecurity Workforce Structure track ensuring that Federal agencies can attract, recruit and retain employees with cybersecurity expertise. The Cybersecurity Workforce Training and Professional Development track is led by the Department of Defense (DOD), the Office of the Director of National Intelligence (ODNI) and DHS to grow expertise of Federal employees.

[12] See Footnote 8.

increasingly valuable information, focusing directly on outcomes. However, it will take time to develop the objectives, determine how capabilities can be implemented to deliver the information, develop supporting standards, work with industry, and provide optimal means to implement those capabilities across the many complex domains that comprise the entire Federal enterprise.

D. Federal Identity, Credential and Access Management

The Cyberspace Policy Review highlighted the importance of identity management in protecting the nation's infrastructure and outlined a number of recommendations. To support this effort, the Federal CIO Council and OMB developed a segment architecture[13] for identity, credential, and access management (ICAM). For the first time, the Federal government has a common government-wide architecture defined to support the enablement of ICAM systems, policies, and processes to facilitate business between the Government and its business partners and constituents. This architecture provides Federal agencies with a consistent approach for managing the vetting and credentialing of individuals requiring access to Federal information systems and facilities.

The implementation of ICAM is leading to several benefits including: increased security; improved compliance with laws, regulations and standards; improved interoperability; enhanced customer services; elimination of redundancy; and increased protection of personally identifiable information. ICAM improves information security posture across the Federal government through standardized and interoperable identity and access controls. The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies.

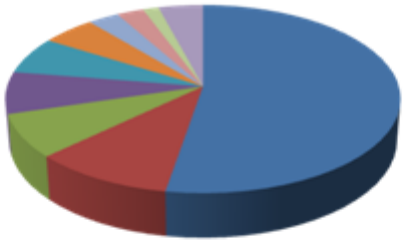
The private sector, other levels of government, and the general public have an equal need for improved digital identification in many cyberspace transactions. To address this issue the Administration developed the National Strategy for Trusted Identities in Cyberspace (NSTIC). To be released in early 2011, the NSTIC will promote 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 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.

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

III. Security Incidents and Response in the Federal Government

The United States Computer Emergency Readiness Team (US-CERT) receives computer security incident[14] reports from the Federal government, State/Local governments, commercial enterprises, U.S. citizens and foreign CERT teams. During FY 2010, US-CERT processed 107,439 incidents as categorized in Figure 2.[15]

Figure 2. Summary of Total Incidents Reported to US-CERT in FY 2010



Phishing	56,579	52.7%
Virus/Trojan/Worm/Logic Bomb	11,001	10.2%
Malicious Web Site	7,971	7.4%
Non Cyber	7,741	7.2%
Policy Violation	6,888	6.4%
Equipment Theft/Loss	5,395	5.0%
Suspicious Network Activity	3,121	2.9%
Attempted Access	2,712	2.5%
Social Engineering	1,571	1.5%
Others	4,460	4.2%
Total	107,439	100.0%

Source: US-CERT

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 Federal-only incident number indicated that the Federal incidents trend was up approximately 39% from FY 2009, even when the overall incidents trend was down approximately 1% for the same period:
    - In FY 2009, US-CERT received a total of 108,710 reports. Approximately 30,000 of those were Federal incidents.

[14] An 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.

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

- In FY 2010, US-CERT received a total of 107,439 reports. Approximately 41,776 of those were Federal incidents.

- Malicious code through multiple means (e.g., phishing, virus, logic bomb) continues to be the most widely used attack approach. As indicated in Table 1, which includes a breakout of incidents reported to US-CERT by Federal agencies in FY 2010, malicious code accounted for 31% of total incidents reported by Federal agencies:

Table 1. Incidents Reported to US-CERT by Federal Agencies in FY 2010

Incidents Category	# of Incidents	% of Total Incidents
Unauthorized Access	5,775	13.8%
Denial of Service	23	0.1%
Malicious Code	12,864	30.8%
Improper Usage	7,329	17.5%
Scans, Probes, and Attempted Access	4,419	10.6%
Under Investigation / Other	11,336	27.2%
Total	41,776	100.0%

- There were repeated attacks on zero-day vulnerabilities[16] through social engineering. Attackers from criminal entities and other actors aggressively exploited zero-day vulnerabilities in applications and products throughout the year. Exploit codes for these vulnerabilities often became publicly available, which placed Federal agencies, private organizations, and individuals at increased risk. These attacks typically require social engineering to trick users into visiting compromised web sites hosting malware or opening a malicious attachment to execute the malware on a user's system.

To address vulnerabilities and to secure government information and computing environments, the Federal government continues taking significant security measures to prevent and process security incidents. US-CERT issued multiple products to Federal and private sector partners to help prevent and mitigate zero-day exploitation activities. These products often included information gathered through analysis of suspicious traffic detected via the Einstein system.[17]

[16] A "zero-day vulnerability" is a vulnerability that is unknown to others or undisclosed to the software developer.

[17] As an example of how US-CERT responds to threats through multiple channels, in September 2010, malware spreading via spoofed e-mail impacted multiple organizations across the public and private sectors. US-CERT alerted public and private sector stakeholders to the malware campaign, advised users to adhere to standard preventive measures, and provided extensive analysis of the malware to them. After deploying Einstein signatures, US-CERT monitored for the malware's continued activity throughout the Federal government and worked with impacted agencies to mitigate the infections.

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.

Besides normal operations, US-CERT participated in the Cyber Storm III exercise along with multiple public, private, and international organizations at the end of FY 2010. The weeklong event evaluated participants' operational capabilities and information sharing practices against an escalating scenario of simulated cyber attacks. While participating in the Cyber Storm III exercise, US-CERT also handled 1,226 real-world incidents that week.

The Federal government continued to sponsor research and development of an Insider Threat assessment methodology and corresponding mitigation strategies through the US-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.

Lastly, in late FY 2010, an interim version of the National Cybersecurity Incident Response Plan (NCIRP) was published, which clearly delineates roles and responsibilities in the event of a major cyber incident and provides an actionable framework for response. The NCIRP establishes the foundation for incident response capabilities across the Federal government.

IV. Key Security Metrics

In FY 2010, agencies continued to be largely in compliance with the requirements of FISMA as measured by the traditional metrics: maintaining a high percentage of systems with security authorizations; training the workforce in basic annual security awareness; and reporting incidents to the proper authorities. However, this reporting cycle is the first time that agencies reported on the newly introduced security performance measures. The new metrics provide wider insight into critical areas such as vulnerability management, incident response, and configuration management.

In many cases, agencies had not previously tracked security performance using the metrics that were requested for this reporting cycle. Therefore, we anticipate that the quality of these metrics will improve significantly over time, as agencies continue the shift to continuous monitoring. As part of this shift, we expect agencies to increase the use of automated security management tools and automated approaches to report security performance information.

Additionally, for the first time, 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 implementation costs. While agencies did report some cost information last year, this reporting cycle represents the first time that detailed security cost information has been officially incorporated into agency budget submissions.

The following sections highlight selected security metrics for FY 2010 for the Chief Financial Officers Act of 1990 (CFO Act)[18] agencies unless otherwise noted. All data are as reported by agencies.[19] Where agencies require improvement in particular areas, the Cyberscope and Cyberstat processes, discussed in Section VI, will be leveraged to improve agency performance.

A. Information Security Metrics

Federal Identity Management

Both *The Cyberspace Policy Review*, issued by the President, and the President's Budget for FY 2012 highlighted the importance of identity management in protecting the nation's infrastructure. Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Employees and Contractors," 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

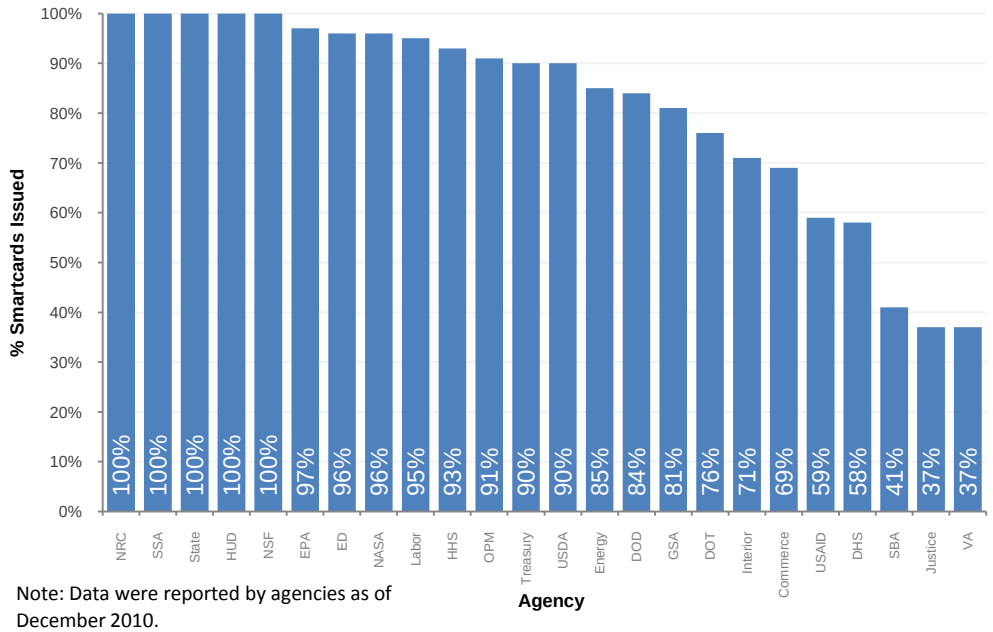
[18] The Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576). See Appendix C for the list of agencies subject to the CFO Act. The agencies on this list are often used as a focus group to review implementation of Federal laws and guidance; including the implementation of FISMA.

[19] Agency names have been anonymized unless the information has already been made public.

standardized credentials required by HSPD-12 include secure access to Federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities.

As of December 1, 2010, agencies reported that more than 4.5 million credentials (79% of the total required to receive credentials) were issued to the Federal workforce (including both government employees and contractors) and almost 5 million background investigations (87% of the total required to have investigations) were completed in accordance with HSPD-12. Figure 3 below summarizes the credential issuance progress by agency.

Figure 3. Smartcard Issuance Progress Reported by Agencies[20]



Note: Data were reported by agencies as of December 2010.

With the majority of the Federal workforce now possessing the credentials, agencies are in a position to accelerate the use of the credentials. While FISMA metrics data indicates that 55% of government user accounts were configured to require PIV credentials to authenticate to agencies' systems, only 2 agencies reported making significant progress in this area and most agencies reported very little progress. For example, one agency reported that 90% of user accounts were configured to require PIV credentials to authenticate to agencies' systems, and another agency reported that 83% of user accounts were configured to require PIV credentials to authenticate to agencies' systems. The remaining 22 agencies reported that between 0% and 3% of user accounts required PIV credentials to authenticate to agencies' systems. Although these agencies do not require the use of the PIV smartcard credentials for access to systems, many have pilot

[20] Agency smartcard issuance progress is available at http://www.idmanagement.gov and http://www.whitehouse.gov/omb/egov.

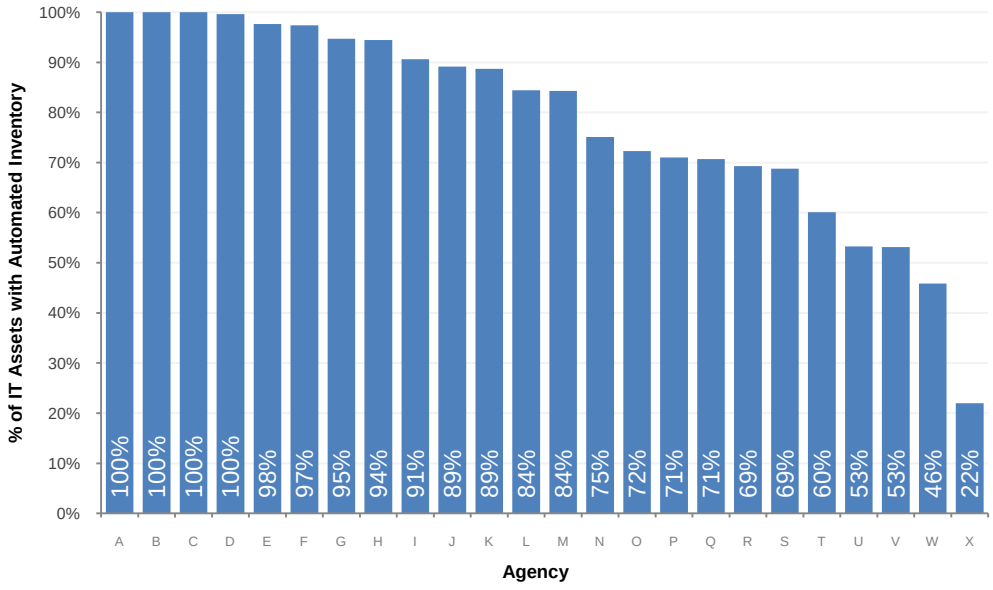
implementations underway. On February 3, 2011, OMB and DHS issued memoranda[21] outlining a plan of action for agencies to expedite the use of PIV credentials.

Implementing Automated Monitoring

Working to automate configuration and vulnerability management has been a top priority in FY 2010. As a result of the leadership from NIST, the National Security Agency (NSA) and the Federal CIO Council, evaluation of systems using automated tools is increasingly being adopted by the public and private sectors alike.

The ideal goal of the IT asset management capability is to have 100% of agency assets under an automated asset management system that captures the necessary data about each asset and can provide that data within a short period of time. This capability enables many other more complicated capabilities, including configuration management and incident response. Agency-reported data indicate that about 66% of IT assets at agencies are being managed with an automated asset management capability. Figure 4 provides the percentage of IT assets with automated capacity for asset inventory, as reported by Federal agencies.

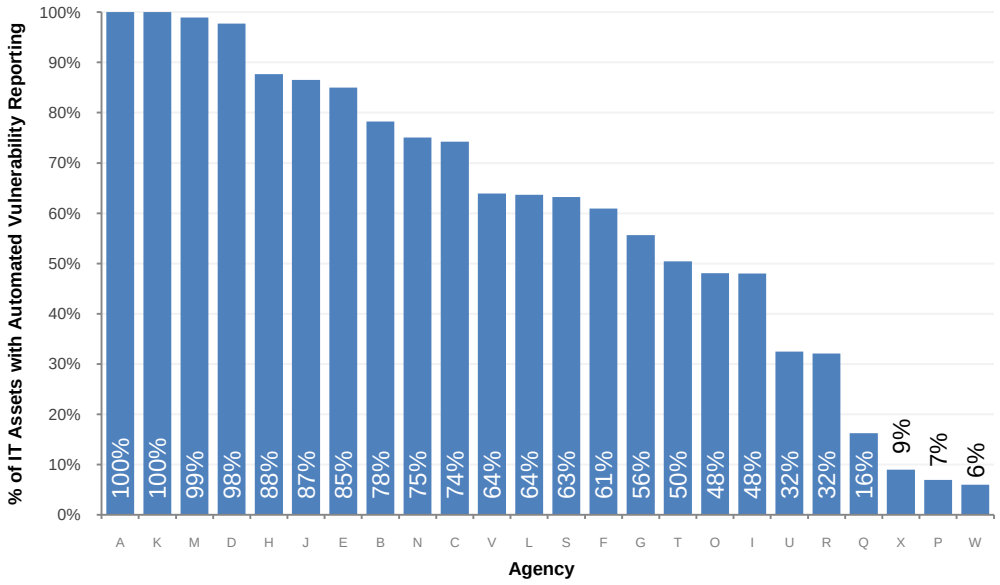
Figure 4. Percentage of IT Assets with Automated Inventory Capability Reported by Agencies



[21] OMB M-11-11: *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*. For a copy, refer to: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

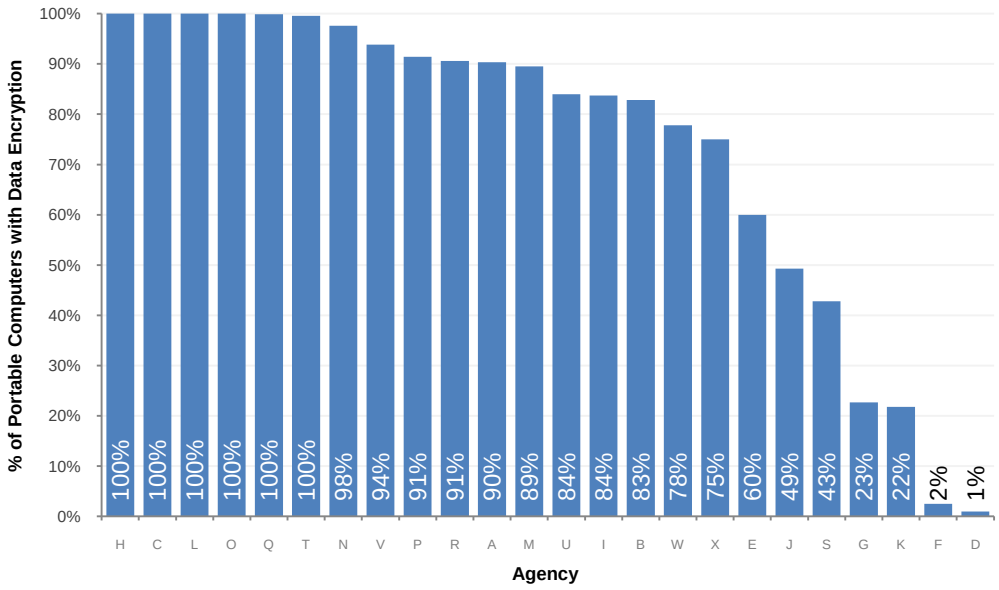
Agencies are also making progress in the use of automated vulnerability management systems that scan agency IT assets for common vulnerabilities (software flaws, required patches, etc.) and facilitate remediation of those vulnerabilities in a short period of time. At present, analysis of the vulnerability management capability across the government shows about 51% of assets are being managed with an automated vulnerability management capability. Figure 5 illustrates the percentage of IT assets with automated access to detailed vulnerability information by agency.

Figure 5. Percentage of IT Assets with Automated Vulnerability Reported by Agencies



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 FIPS 140-2 validated encryption. Agencies have reported good progress in implementing this capability. The government-wide average is 54% with several agencies having achieved 100%. Figure 6 illustrates the percentage of portable computers[22] with FIPS 140-2 encryption by agency, as reported by agencies.

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



Incident Response and Reporting

On average, it takes agencies almost 9 hours to determine whether anomalous behavior is an actual incident. The time between detection and reporting has a major impact on incident handling for US-CERT. Based on agency reports, this period is on average 20 hours.

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 mature significantly over the next year and, as other capabilities mature, will keep improving. In addition, US-CERT is making significant strides in increasing communication with agency Network Operation Centers (NOCs) and Security Operation Centers (SOCs) and providing more specific and actionable information relevant to each agency, further enhancing this capability government-wide.

[22] Under the category of portable computers, most agencies reported the encryption percentage of laptops, while a few agencies reported the encryption percentage of laptops and other mobile devices, such as personal digital assistant devices and blackberries.

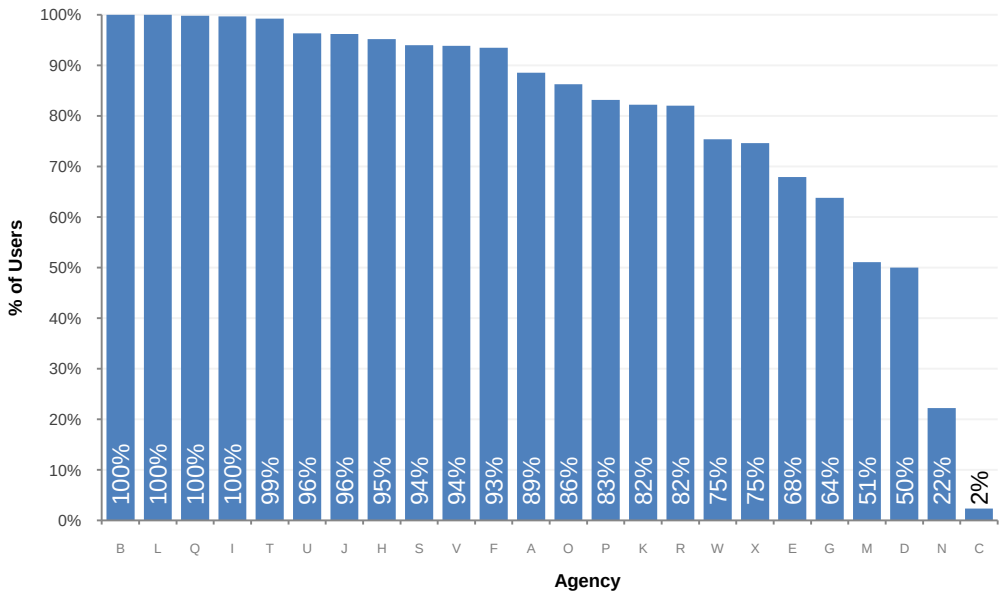
Security Training

Training continues to hold significant importance in addressing challenges associated with protecting our networks, systems, and data. Given the prevalence of phishing attacks and the continual evolution of adversary tactics, techniques, and procedures, the frequency with which users and security professionals receive effective training and education must be increased and the content continually refreshed. The baseline data collected this year will be used to identify feasible goals in this area, drive appropriate policy, and provide insight into potential solutions we can collectively pursue.

Agencies are generally meeting the annual requirement for cybersecurity awareness training, with about a third providing it with a frequency of every 30 days or less and a few, as a best practice, providing daily supplemental security training.

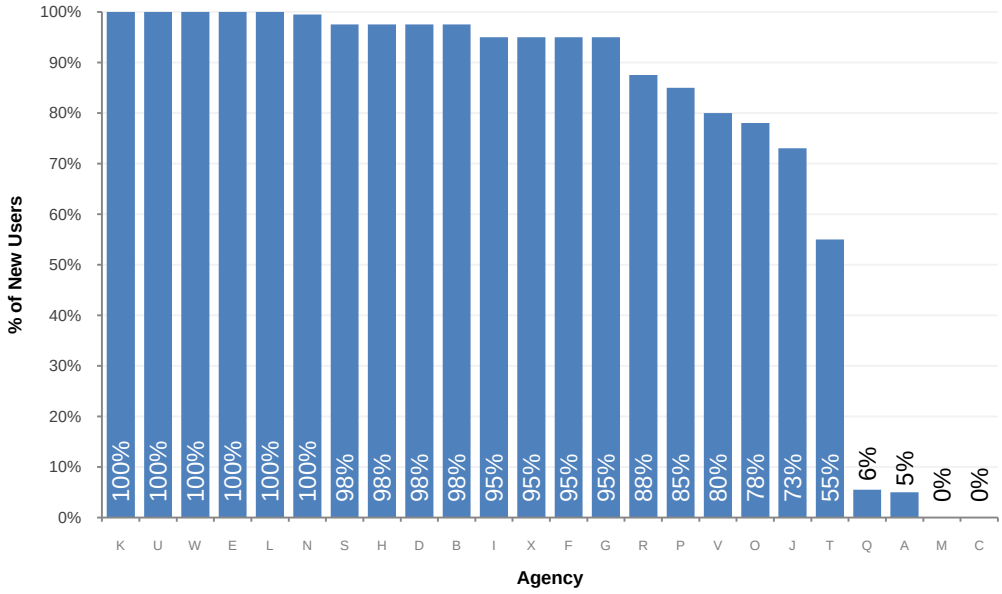
Specialized cybersecurity training for agency users with significant security responsibilities averages 88% across all Federal agencies. Figure 7 provides by agency the percentage of agency users with significant security responsibilities given specialized annual cybersecurity training.

Figure 7. Percentage of Users with Significant Security Responsibilities Given Specialized Annual Security Training Reported by Agencies



Agencies reported that 73% of new users were given security awareness training prior to being granted network access. Figure 8 provides, by agency, the percentage of new users completing security awareness training before being given network access.

Figure 8. Percentage of New Users Completing Security Awareness Training Before Being Given Network Access 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 Circular A-11 (2010) Section 53 introduced a major change for the FY 2012 budget cycle by adding an Exhibit 53B Agency IT Security Portfolio that requires agencies to report IT security cost and budget data. Beginning in the FY 2012 budget cycle, the Exhibit 53B requires agencies to report agency IT security portfolio information for the Prior Year, Current Year, and the Budget Year. As part of their Exhibit 53B submissions, agencies reported cost information in areas such as IT security testing, security tools, assessment and authorization, training, and personnel.

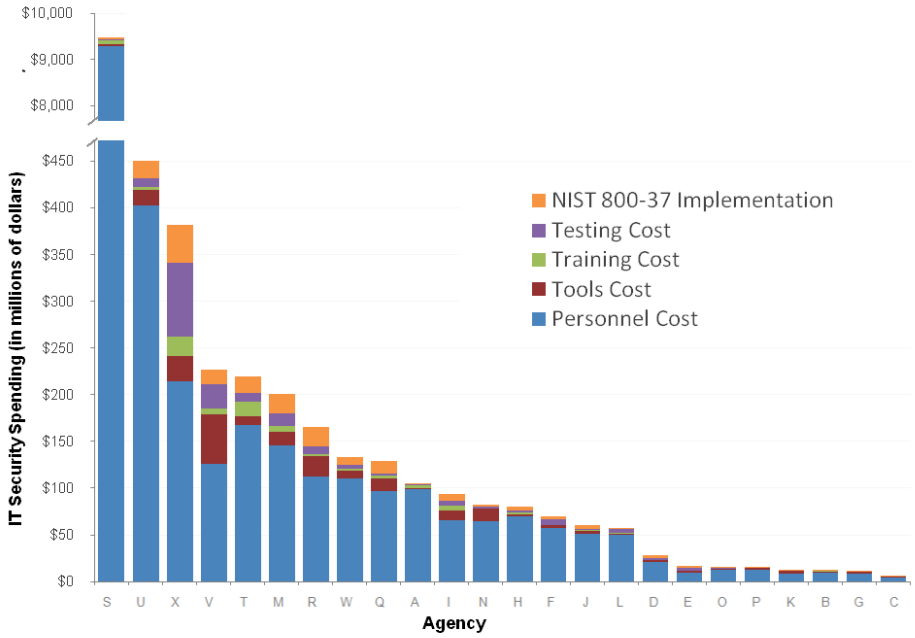
This section of the FISMA report provides the IT security cost analysis based on the Exhibit 53B data for FY 2010.[23] This is the first year of using this set of Exhibit 53B metrics to collect IT security cost data; therefore, the historical comparison on IT security cost trends is not available. Additionally, this section focuses on data reported by the CFO Act agencies and does not include data reported by small and micro agencies.

[23] 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 as required by OMB Circular A-11.

IT Security Spending for Agencies

In FY 2010, the CFO Act agencies reported total IT security spending of $12.0 billion. Figure 9 provides the agency-reported IT security cost by spending category.

Figure 9. IT Security Spending Reported by Agencies



The total IT security cost includes cost categories for direct spending such as costs for security personnel[24], tools, testing, training, and NIST SP 800-37 implementation. [25]

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.

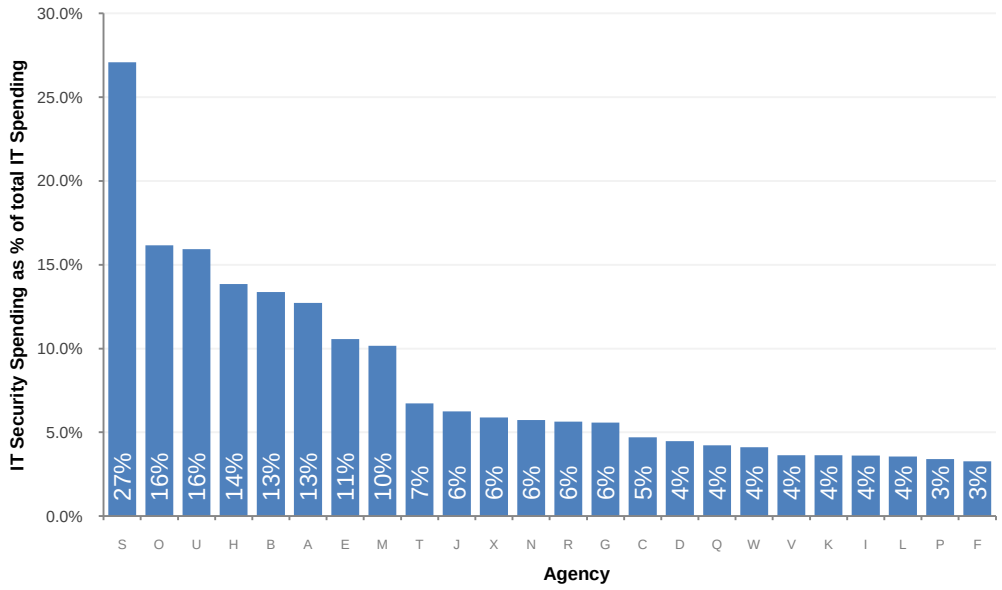
The indirect costs of IT security are very difficult to separate from other operational and managerial costs. However, it should be noted that direct costs are only part of the total IT security costs spent by an agency.

[24] DOD indicated that the majority of its IT workforce is in the category of "personnel with significant information assurance responsibilities." DOD stated that their IT security costs include costs for both IT and information assurance personnel to account for those with privileged access, etc.

[25] NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

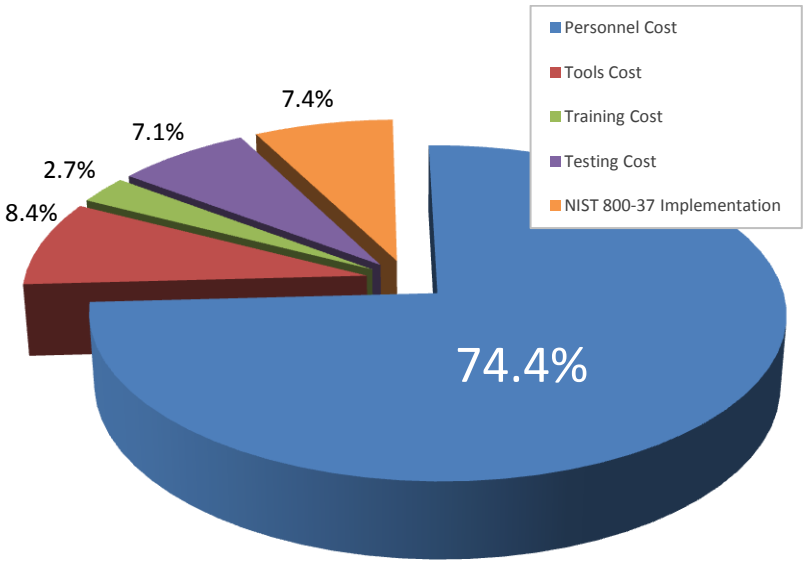
Figure 10 shows the percentage of FY 2010 IT spending that was for IT security. Overall, 15.6% of agencies' IT spending was spent on IT security. CFO Act agencies spent a range of 3% to 27% of their total IT budget on IT security.

Figure 10. IT Security Spending as a Percentage of Total IT Spending Reported by Agencies



In FY 2010, 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 74% of their IT security costs on personnel, as indicated in Figure 11 below.

Figure 11. Percentage Breakout of IT Security Costs by Category Reported by Agencies



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

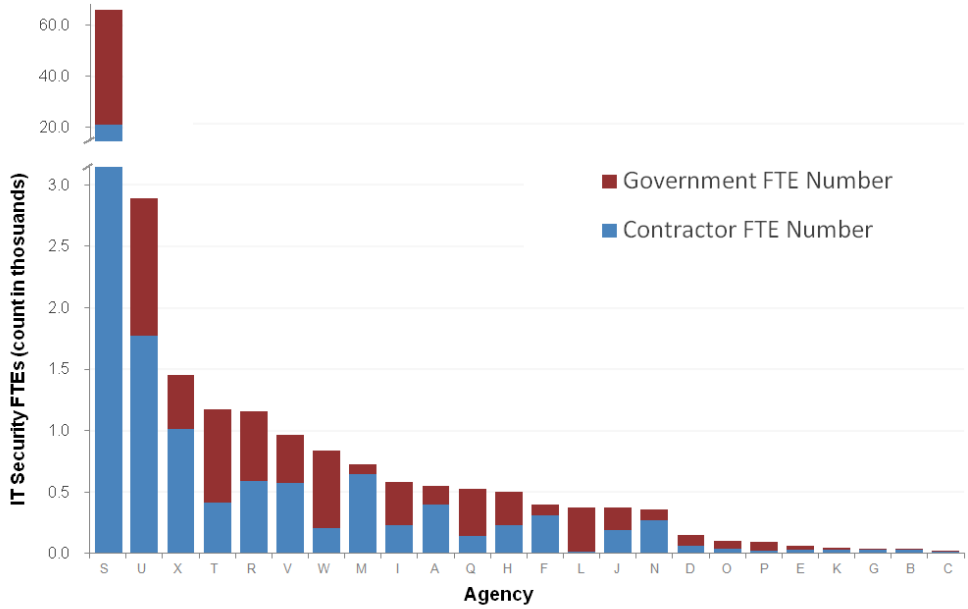
As further indicated by Figure 11, of the reported IT security costs government-wide, agencies spent 8% on security tools, 7% on NIST 800-37 implementation, 7% on security testing, and 3% on security training. NIST 800-37 requires agencies to apply the Risk Management Framework to Federal information systems using a Security Life Cycle Approach, advancing from the previous periodic 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 cost-effective strategies in IT security spending. This workforce-enabling strategy requires going beyond technical trainings to include process improvement, innovation encouragement, collaboration mechanisms, and accountability structures.

Personnel Costs

In FY 2010, CFO Act agencies reported a total of 79,434 Full Time Equivalents[26] (FTEs) with major responsibilities in information security. Figure 12 provides a breakout of Total IT Security FTEs by agency.

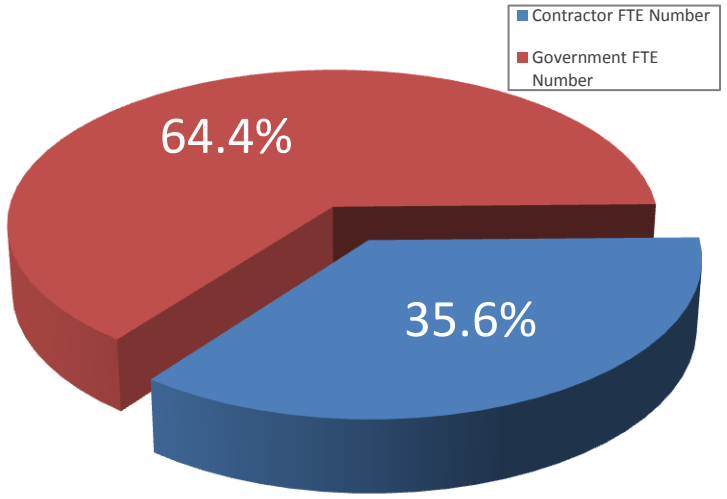
Figure 12. Total IT Security FTEs Reported by Agencies



[26] 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, 64% are government FTEs, 36% are contractor FTEs (Figure 13). This percentage is heavily influenced by DOD's large FTE numbers. DOD's IT security personnel are 68% government FTEs and 32% contractor FTEs. Excluding DOD, 46% of security FTEs are government FTEs, and 54% are contractor FTEs. IT security has consistently been a functional area that depends on talent and technical expertise from industry and commercial sources.

Figure 13. Percentage of Government FTEs Compared to Contractor FTEs



C. 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 ten areas:

- Security Authorization[27]
- Security configuration management
- Incident response and reporting
- Security training
- Plans of actions and milestones (POA&M)
- Remote access
- Account and identity management
- Continuous monitoring
- Contingency planning

[27] In the guidance issued to the IGs for FY 2010, this was referred to as Certification and Accreditation. With the release of NIST Special Publication 800-37 in February 2010, the term Certification and Accreditation was eliminated.

- Oversight of contractor systems

By considering 62 attributes pertaining to the ten areas, the Inspectors General (IGs) determined one of three levels for the agency: (1) the agency had established and maintained a program that was generally consistent with NIST and OMB 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. The IGs were also asked, to the extent they determined that the agency's program for a certain security area needed significant improvements, to identify the needed improvements from a standard list of possible problem issues for each of the ten areas. If an IG identified an improvement needed in an area that was not on the area's list of issues, he or she was asked to provide a narrative describing the issue and the needed improvements.

Table 2 summarizes the results from the IGs of the 24 CFO Act agencies by information security program area. Based on these results, the agencies performed best in security authorization, incident response and reporting, and remote access. Their weakest performance occurred in continuous monitoring, oversight of contractor systems, configuration management, security training, and account and identity management.

Table 2. Overall IG Findings for the 24 Agencies by Information Security Area

Cyber Security Program Area	Compliant Program		Needs Improvement		Program Not Implemented	
	No.	%	No.	%	No.	%
Security Authorization	13	54	11	46	0	0
Configuration Management	6	25	18	75	0	0
Incident Response	15	62	9	38	0	0
Security Training	7	29	17	71	0	0
POA&M	8	33	16	67	0	0
Remote Access	10	42	14	58	0	0
Account and Identity Management	5	21	19	79	0	0
Continuous Monitoring	7	29	15	63	2	8
Contingency Planning	8	33	16	67	0	0
Contractor Oversight	6	25	16	67	2	8

Table 3 provides the 24 agencies' compliance scores[28]. Only one agency received a compliance score of 100% for its information security program which, based on its IG's review, met all 62 attributes. The remaining agencies had at least one area that needed improvement. Three agencies did not have a cyber security program in place for one security area, and one agency did not have a program in place for two security areas. Total numbers of areas with deficiencies were used to compute compliance scores. Six agencies scored over 90% compliance, eight scored between 65 and 90% compliance, and the remaining nine scored less than 65%.

Table 3. CFO Act Agencies Compliance Score Based on IG Reviews

Agency	Compliance Score
Agency L	100.0%
Agency P	99.2%
Agency B	98.9%
Agency E	96.7%
Agency X	92.5%
Agency G	90.4%
Agency D	87.6%
Agency K	87.3%
Agency T	86.4%
Agency U	85.8%
Agency M	84.6%
Agency N	79.4%
Agency R	77.9%
Agency A	71.9%
Agency V	64.7%
Agency F	60.8%
Agency O	57.8%
Agency W	57.0%
Agency C	50.3%
Agency H	44.5%
Agency Q	29.8%
Agency J	24.6%
Agency I	13.7%
Agency S	N/A*

*Agency S' IG did not provide sufficient information to score.

[28] The IG method for calculating the score in Table 3 is as follows:
Each of the 10 cyber security program areas was assigned a value of 10 points for a total of 100 possible points. For areas where the respective OIGs answered "A", the agency received the full 10 points. When OIGs answered "B", the agency received a prorated score based on the number of deficiencies noted. When OIGs answered "C", the agency did not receive any points in that area.

The more specific IG evaluation results can be found in Appendix 1.

V. Progress in Meeting Key Privacy Performance Measures

Ensuring the privacy of personal information for all Americans remains a top Administration priority. 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. Agencies have been reviewing their information systems to ensure that they eliminate unnecessary holdings of personally identifiable information (PII) such as unnecessary collection and use of Social Security numbers (SNNs). In addition, Federal agencies continued developing and implementing policies, rules of behavior, training for all personnel and key staff, and corrective actions to address non-compliance. Agencies have been working with their Senior Agency Officials for Privacy (SAOP) to ensure that all privacy impact assessments and system of record notices (SORNs) are completed and up-to-date. Federal agencies also continued to implement appropriate data breach response procedures.

As discussed in the sections that follow, the FY 2010 agency FISMA reports indicate general improvements in most privacy performance measures.

Table 4. Status and Progress of Key Privacy Performance Measures

	FY 2008	FY 2009	FY 2010
Number of systems containing information in identifiable form	3,505	4,266	3,855
Number of systems requiring a Privacy Impact Assessment (PIA)	2,002	2,605	2,304
Number of systems with a PIA	1,850	2,319	2,135
Percentage of systems with a PIA	**92%**	**89%**	**93%**
Number of systems requiring a SORN	2,373	3,373	2,997
Number of systems with a SORN	2,205	3,243	2,870
Percentage of systems with a SORN	**93%**	**96%**	**96%**

Privacy Program Oversight

In FY 2010, 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 all 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 2010, 93% of applicable systems across the 24 CFO Act agencies had publicly posted PIAs, an increase from 89% in 2009. The increase in PIA compliance occurred as the number of systems requiring a PIA decreased slightly.

Written Policies for Privacy Impact Assessments

In 2010, all 24 agencies reported having written policies in place for the following topics:

- Determining whether a PIA is needed;
- Conducting a PIA;
- Evaluating changes in technology or business practices that are identified during the PIA process;
- 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.

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 2010, 96% of information systems government-wide with Privacy Act records have published current SORNs. This is the same compliance percentage as 2009, while the number of applicable systems decreased slightly.

Privacy-Related Policies and Plans

On May 22, 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* which requires agencies to:

- Develop and implement a breach notification plan;
- Develop and implement a plan to eliminate unnecessary collection and use of Social Security numbers in agency programs;
- Develop and implement a plan to review and reduce unnecessary holdings of personally identifiable information ; and
- Develop and implement a policy outlining rules of behavior for agency employees and identifying consequences and corrective actions available for failure to follow these rules.

The requirements established in M-07-16 have played a critical role in agencies' efforts to safeguard PII. Since the issuance of M-07-16, agencies have demonstrated progress in establishing and revising breach notification plans, which has provided a better foundation for responding to potential breaches. For example, agencies have developed model documents, such as sample breach notification letters, along with the plans for rapid response in the event of a breach. These efforts continue.

Agencies have also continued their efforts to develop rules of behavior to sensitize agency officials to the privacy risks associated with collection and retention of SSNs and other PII. However, specific activities vary across agencies, and these efforts will require ongoing oversight through the capital planning process, Paperwork Reduction Act reviews[29], Executive Order 12866[30] regulatory reviews, and other oversight mechanisms. In order to facilitate agency SSN reduction efforts, Executive Order 13478, *Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers*, removed a requirement for agencies to use SSNs as individuals' unique identifiers.

[29] Paperwork Reduction Act of 1995 (44 U.S.C. 3501), PUBLIC LAW 104-13.

[30] Executive Order 12866 of September 30, 1993, *Regulatory Planning and Review*.

VI. Path Forward

The main priority in Federal information security for FY 2011 will be to build a defensible Federal enterprise that allows the Federal government to have information security as a key enabler instead of a limiting factor in harnessing technological innovation. For too long security has been a barrier for new technologies in government, creating an increasing disconnect between agencies and the people they serve. Fixing this problem will not happen overnight; it will require a vigorous and extensive build-out of technical and policy protection mechanisms for government systems, a growing and robust partnership with the private sector, and a focus on interagency cooperation. Below are the pillars of this approach.

A. Continuous Monitoring and Remediation

In FY 2011 the shift from the once-a-year FISMA reporting process to a monthly reporting of key metrics through Cyberscope will allow security practitioners to have more information than ever before to assist the protection of agency information and information systems. In the years to come, this reporting will require minimal human interaction and allow immediate remediation of many vulnerabilities.

While automation efforts such as the Security Content Automation Protocol (SCAP)[31] and continuous monitoring are not magic solutions, they do offer enterprises of all sizes the ability to enhance one's security posture at lower costs. This work has begun to pave the way for new and robust capabilities that agencies can easily adopt in the future. Applying the continuous monitoring and remediation approach must be coupled with an increased engagement across government and industry to better cooperate to address information security.

Strengthening Security Management through CyberStat Model

To increase this cooperation, in January 2011, DHS launched CyberStat. Using the TechStat[32] model, DHS cybersecurity experts will now meet with agencies regularly to ensure accountability and to help agencies develop focused actions plans to improve their information security posture. CyberStat is grounded in the data provided by CyberScope, among other key data sources about agencies' information security. The development of clear and consistent metrics for CyberScope has increased the ability of DHS to hold agencies accountable for outcomes. As DHS works with agencies to improve data quality, CyberStat and CyberScope will allow DHS to assist agencies in quickly addressing problems that pose risks.

B. Hardwiring Security from the Beginning

Recognizing that the best security is "baked in" to IT investments and not added after the investments have been deployed, DHS needs to determine where in the life cycle development of

[31] NIST Special Publication (SP) 800-126 defines Security Content Automation Protocol (SCAP) as a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information.

[32] A TechStat accountability session is a face-to-face, evidence-based review of an IT program between OMB and agency leadership, powered by the Federal IT Dashboard and input from the American people. (see http://www.whitehouse.gov/blog/2010/02/24/techstat-improving-government-performance.)

systems agencies are spending their resources. The information collected for FY 2010 through agencies' FY 2012 budget submission is the initial step in obtaining this crucial cost data. In the coming years, access to continually refined cost data will allow better evaluations of the efficiency of Federal government expenditures on security. The collection of detailed information, especially when combined with performance-based metrics, will allow agencies to make informed, risk-based decisions on where to allocate scarce resources.

Designing into Workflow and Technology

Designing security and privacy controls into workflows, systems, infrastructures, facilities, and enabling technologies is a critical success factor for achieving effective levels of protection and resiliency. Establishing and maintaining enterprise-wide, integrated business and technology architectures that cover both the classified and unclassified information sharing domains is the essential starting point to achieve required levels of confidentiality, integrity, and assurance. The architecture provides the context and standards for analysis, design, and documentation activities throughout the lifecycle of information security controls. In this way, security solutions can be "hard-wired" into business and technology capabilities. The following initiatives will be further deployed in FY 2011 and will allow security to underpin all the activities of these agencies.

Over the past 2 years, NIST has led a number of discussions with civilian, military, and intelligence agencies that promoted a convergence of thinking on security controls and risk management.[33] In December 2010, NIST also released a new draft of vulnerability naming schemes, which will help to further standardize how security is designed into processes, systems and infrastructure across the Federal government.

In May 2010, the Federal CIO Council released version 3.0 of the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) that for the first time linked together security, privacy, and architecture best practices to support the effective design, implementation, and use of security and privacy controls in unclassified and classified information systems. The FEA-SPP release also included an analytic tool for civilian, military, and intelligence agencies to use to be able to identify the controls needed in systems at the low, moderate, and high levels of information sensitivity in both the unclassified and classified information sharing domain.

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

[33] These discussions were the source of important input for the Risk Management Framework (SP-800-37) and its incorporation in December 2010 to SP-800-39 to create "Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View." In August 2009, revision 3 to SP-800-53 was released, which provided an updated list of security controls that are central to hard-wiring protective capability.

performance, reduce overall costs, and increase efficiency 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 2010, ISSLOB established an updated set of requirements for Risk Management Framework services, based upon the updated NIST SP 800-37 Revision 1, with the goal of establishing a Blanket Purchase Agreement (BPA) with private sector vendors. The ISSLOB Risk Management Framework BPA, leveraging the GSA Smartbuy Program, is currently in the award phase. The objective of this acquisition will be to award multiple BPAs for managed service providers capable of providing Risk Management Framework capabilities.

Also in FY 2010, 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 $7.6 million in cost savings during the initial year of availability versus standard GSA pricing for the same information security products. Furthermore, the estimated cost savings do not include the cost avoidance associated with conducting requirements development, providing for acquisitions centrally as compared to at each and every agency, nor does it include the effectiveness of ensuring that all security procurements of this type adhere to critical standards such as SCAP.

Additionally, in FY 2010, ISSLOB began executing and planning of the SAIR TIER II & Continuous Monitoring BPAs and will continue to work with its acquisition and Federal civilian agency partners to award the BPAs in FY 2011. These BPAs will deliver an economical means to implement continuous monitoring capabilities across the Federal enterprise.

Standardizing Security through Configuration Settings

Secure configuration settings allow agencies to reduce risks across their enterprise by deploying settings that are more restrictive than what the manufacturer provides out of the box. When properly implemented, they reduce the risk of exploitation of yet-to-be discovered vulnerabilities as well as current risks. After deploying standard configuration settings, agencies can more effectively monitor their systems and deploy patches when needed.

This year, 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 security configurations for all agencies. Agencies will make risk-based decisions as they customize this baseline to fit their needs. In many cases this means implementing more secure settings.

Moving forward, updated settings may be provided for these products to account for unforeseen challenges or upgrades. In addition to such modifications, in FY 2011 the USGCB will evaluate additional products to allow for increased deployment of secure settings across the Federal enterprise.

Establishing a Working Group to Prevent the Purchase of Counterfeit Products

The Comprehensive National Cybersecurity Initiative (CNCI) was launched in 2008 with the issuance of National Presidential Directive 54 and Homeland Security Presidential Directive 23. In 2009, the Administration determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI activities include *CNCI Initiative 11: Develop a multi-pronged approach for global supply chain risk management.*[34]

In support of CNCI Initiative 11, OMB has been working with the National Aeronautics and Space Administration (NASA), GSA, and DOD to develop a strategy to address the procurement of counterfeit goods, including IT, by the Federal government. DOD and NASA both have significant concerns involving counterfeits entering the supply chain, which could potentially compromise the health and safety of our troops, astronauts, and numerous other Federal government personnel. Both agencies have been assessing their issues internally, have taken steps to develop procedures and practices to identify, detect, prevent, report and safeguard against the purchase of counterfeit products, and agree that a Federal government-wide approach to addressing this problem is warranted.

As a result, OMB, DOD, NASA and GSA have partnered to identify areas of common interest and compare progress and best practices to ultimately eliminate counterfeits in their supply chains. The objective of this partnership is to develop a framework which will form a consistent government-wide approach for reducing the Federal government's vulnerability to counterfeits that is flexible enough to accommodate the wide variety of missions across Federal agencies. As part of this collaboration, DOD, NASA, GSA and other agencies, as appropriate, will form a working group to identify any gaps in legal authority, regulation, policy and guidance that preclude an optimal Federal government procurement approach.

C. Enabling the Secure Adoption of New Technologies

The Administration is also working aggressively to ensure that we can bring new technology into the government more rapidly and more securely.

Empowering a Mobile Workforce with Wireless Security

The Administration is committed to expanding mobile and wireless platforms, applications, and tools to provide the American people and Federal employees access to governmental information, services, and resources when, where, and how they want them. As mobile and wireless becomes more ubiquitous inside and outside of government, security becomes even more critical.

Many challenges are presented by interconnecting a wide variety of wired and wireless networks, which often are not interoperable. The challenges include addressing the security and privacy

[34] *The Comprehensive National Security Initiative*. http://www.fbiic.gov/public/2010/mar/CNCIUnclassifieddescriptionfinal.pdf

implications of seamless mobility and developing methods for correcting security and privacy issues. Appropriate security and privacy precautions must be part of agency strategic planning. Threats caused by inherent vulnerabilities of mobile/wireless networks must be identified. Implementing remedial solutions must be part of the strategy. In FY 2011 security standards for government use of mobile/wireless devices, applications, platforms, and networks will be established and updated.

Protecting Privacy and Security in Health IT

To guide evolving technology, careful attention to privacy and security policies at the Federal and State levels is needed to ensure that nationwide interoperable Health IT (HIT) is achieved with a high degree of public confidence and trust. The adoption of baseline and common confidentiality, privacy, and security protections is essential to building that trust among involved patients and other stakeholders. Application of these protections by entities engaged in electronic exchange of health information can help foster the adoption of HIT. Addressing many of the policy issues regarding electronic disclosure, access, and use of health information, while ensuring that privacy, security and civil liberties protections are in place, will facilitate the electronic exchange, access, and use of health information for health care delivery. To accomplish this, during FY 2011-12 the HIT community will focus on:

- Assuring the integrity of the health information being exchanged, accessed, and used by providers and patients, which can lead to higher quality care. Establishing national principles for health information security and stewardship will allow providers to trust that the information they use when assessing and treating patients is as accurate as possible and has not been accessed by unauthorized users.
- Harmonizing privacy and security policies across care settings and communities, which can help facilitate the appropriate exchange of health information and increase consistent protections for health information. Providers and patients will be able to easily access and use health information when and where it is needed while being assured that only those who are authorized have access to this information.
- Ensuring that all stakeholders are aware of patient privacy rights, and that patient perspectives are included and addressed when organizations develop privacy and security policies and implementation approaches, which can promote patient-focused care. By involving patients and patient advocates in the policy development process – at Federal, State, local, and organizational levels – all stakeholders will be better informed about patient privacy rights and patient preferences, and this, in turn, will increase trust in nationwide exchange of health information.
- Patient-focused care is dependent on patients having access to their own information. The use of personal health records by health care consumers is expected to increase in proportion to the trust they place in the protections of their information being exchanged electronically.[35]

[35] Federal Health IT Strategic Plan, the Office of the National Coordinator for Health Information Technology: 2008-2012.

Supporting Telework

FY 2011 will see growth in Federal government teleworking, which provides multiple benefits for agencies and Federal employees. It can produce facilities and resource savings for agencies and improve work-life balance for individuals. Telework reduces time, expenses, and greenhouse gas production associated with commuting. Further, it improves the ability of agencies to continue working in the case of an emergency or natural disaster.

If not properly implemented, however, telework may introduce new information security and privacy vulnerabilities into agency systems and networks. To better understand and manage these vulnerabilities, in FY 2010 DHS began collecting performance metrics through Cyberscope specific to telework practices. As the number of Federal employees' teleworking grows in FY 2011 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. Additionally, new guidelines will allow for technical implementation of telework and secure remote access to systems in agency networks.

Ensuring Safe and Secure Adoption of Cloud Computing

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. Cloud solutions, which can be cheaper, deployed rapidly, and are available on demand, enables agencies to approach IT as a service, instead of owning an asset. Savings generated by cloud computing will be reinvested by agencies in their most critical mission needs. In order to increase the adoption of cloud solutions, the Federal government has adopted a "Cloud First" policy. Moving forward, when evaluating options for new IT deployments, agencies will default to cloud-based solutions. However, it is not sufficient to consider only the potential value of moving to cloud services. Agencies should also consider the readiness and potential risks of cloud providers. Cloud security concerns are multidisciplinary and include items such as privacy, civil liberties, data integrity, statutory compliance, data controls and access.

In order to address these cloud security issues from a macro perspective, government-wide solutions have been developed. This includes the Federal Risk and Authorization Management Program (FedRAMP), which has been established to provide a standard approach for security authorization of cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use. 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.

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.

D. Preventing Unauthorized Disclosure

Our national security requires that classified and sensitive government information be maintained in confidence to protect our citizens, our democratic institutions, our homeland, and our international partners. Protecting information critical to our nation's security is the responsibility of each individual and agency that is granted access to this information.

The unauthorized disclosure of classified government information by Wikileaks highlighted the need for increased vigilance. After this incident, every agency that operates classified information systems or networks was directed to conduct a security assessment with counterintelligence, security, and information assurance experts. The assessment utilizes related law and guidance as a baseline and includes process and technical evaluations to ensure that users do not have broader access than that which is necessary to do their jobs effectively, and to examine the need for restrictions on removable media. Based on assessment findings, agencies are required to implement appropriate changes and ensure that proper levels of protection for classified and sensitive information are in place.

With regard to the handling of government information, FISMA requires the head of each 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 agency that is operating or exercising control over national security systems.

To address the Wikileaks incident and changes in policy, procedures, or standards that may be required, the National Security Advisor named Russell Travers on December 1, 2010 to serve as the National Security Staff's senior advisor for information access and security policy. Mr. Travers is currently leading a comprehensive multi-agency effort to identify and develop the structural reforms needed in light of the Wikileaks breach. His responsibilities include facilitating interagency discussions on balancing needs for information sharing and protection, as well as developing options for Deputies, Principals, and the President regarding the need for technological and/or policy changes that his review and agency assessments reveal.

Conclusion

A secure, trusted computing environment in the Federal government is the responsibility of everyone involved from the agency heads to those charged with implementation and oversight. It entails employees, contractors, and the American people working together to create a culture of vigilance and security to enable us to continue to efficiently leverage the power of technology while respecting the privacy and civil liberties of the American people. It will not be easy nor will it take place overnight. These actions in FY 2010 represent important steps towards a stronger defense of the Federal enterprise, but a continued focus is needed to remain ever-vigilant and forward looking.

Appendix 1. Inspectors General's Findings

In FY 2010, each Agency Inspector General (IG) assessed his or her agency's information security programs in the following ten areas:

- Security Authorization
- Security configuration management
- Incident response and reporting
- Security training
- Plans of actions and milestones
- Remote access
- Account and identity management
- Continuous monitoring
- Contingency planning
- Oversight of contractor systems

This appendix provides the detailed results of IGs' assessments for these ten areas.

Security authorization: The Security Authorization program is a key component of Federal information security. OMB requires each system to be authorized to operate – that is, to pass a properly executed assessment and security authorization – at least once every three years and each time it undergoes a significant change. The process is intended to ensure that risks are identified and sufficiently mitigated before a system operates.

In general, the agencies performed well in security authorization, and as shown in Table 2 in the main report, all agencies have area programs. Furthermore, 13 of the 24 agencies have programs that include the attributes that the IGs evaluated. The remaining 11 agencies, however, have programs in place that need improvements. The following deficiencies were the most common:

- Inadequate process to assess security control effectiveness;
- Security plans did not adequately identify security requirements;
- Security authorization procedures were not fully developed, sufficiently detailed, or consistently implemented.

Security configuration management: In order to secure both software and hardware, agencies need to develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. OMB requires all Window XP work stations to conform to government-wide standard configuration settings. In addition, NIST has created a repository of software baselines.

Based on IGs' reviews, security configuration management is one of five areas that need the most improvement. While all agencies have security configuration management programs, 18 agencies' programs need significant improvements. IGs observed the following deficiencies at least 10 agencies:

- Patch management process was not fully developed;
- Configuration-related vulnerabilities had not been remediated in a timely manner;
- Configuration management procedures were not fully developed, sufficiently detailed, or consistently implemented;
- Standard baseline configurations were not fully implemented;
- Software scanning capabilities were not fully implemented;
- Federal Desktop Core Configuration is not fully implemented and/or all deviations were not fully documented.

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 the appropriate authorities. OMB has designated 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. Fifteen IGs reported that their agencies had incident response and reporting programs in place and that the programs were fully compliant with applicable standards. The remaining nine IGs identified areas in need of significant improvement. The most commonly identified deficiencies were:

- Insufficient incident monitoring and detection coverage;
- Incident response and reporting procedures were not fully developed, sufficiently detailed, or consistently implemented;
- Incidents were not identified in a timely manner.

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 protecting information. 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.

While all IGs reported that agencies had security training programs in place, this area was also one of five areas that the IGs identified as needing the most improvement. Seventeen of the 24 IGs identified that significant improvements were needed to be fully compliant with applicable requirements. The following two weaknesses were identified at more than 10 agencies:

- Identification and tracking of employees with significant information security responsibilities was not adequate;
- Less than 90% of employees, contractors, or other users with significant security responsibilities had attended specialized training in the past year.

In addition, eight IGs identified as a weakness that specialized security training procedures were not fully developed or sufficiently detailed.

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 that risk, associated costs, and expected completion dates.

All 24 IGs indicated that the agencies had POA&Ms in place. However 16 IGs also indicated that their agency programs needed significant improvements. Ten or more IGs identified the following four problems:

- POA&Ms did not include all known security weaknesses;
- POA&M procedures were not fully developed, sufficiently detailed, or consistently implemented;
- POA&Ms were not updated in a timely manner;
- Costs associated with remediating weaknesses were not identified.

Remote access: Secure remote access is essential to agency operations. Because remote access has proliferated through telework, mobile devices, and information sharing, information security is no longer confined to system perimeters. Each method of remote access requires protections, such as multi-factor authentication, not required for local access. Agencies also rely on remote access as a critical component of contingency planning and disaster recovery, heightening the need for strong protections over remote access.

While no agency reviewed lacked a remote access program, only 10 of the 24 agencies had fully compliant programs. The remaining 14 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:

- Remote access procedures were not fully developed, sufficiently detailed, or consistently implemented;
- Multi-factor authentication was not properly deployed;
- The agency did not adequately monitor remote devices when connected to the agency's networks remotely.

Account and identity management: Proper account and identity management ensures 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. By requiring the use of Personal Identity Verification (PIV) cards by all agencies, Homeland Security Presidential Directive 12 mandates a major component of a secure, government-wide account and identity management system.

Account and identity management was identified as one of the areas needing most improvement. Only five of the 24 IGs reported that their agency had a fully compliant program in place. The remaining 19 IGs all identified areas of their agencies' account and identity management programs that needed significant improvement. Ten or more IGs identified the following two controls as containing weaknesses:

- Account management procedures were not fully developed, sufficiently detailed, or consistently implemented;
- Accounts were not properly terminated when users no longer required access.

At least seven IGs identified the following four controls as weaknesses:

- The agency did not use multi-factor authentication where required;
- Privileges granted were excessive or resulted in capability to perform conflicting functions;
- The agency did not use dual accounts for administrators;
- Network devices were not properly authenticated.

Continuous monitoring: The practice of full system security assessments during recertification every third year with limited annual retests has given way to continuous monitoring and adjustment of security controls because 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 of any area programs. Two agencies entirely lack continuous monitoring programs, while seven IGs reported that their agencies' programs were fully compliant, and 15 others needed to implement significant improvements to make their programs fully compliant. Of those 15 agencies, at least 10 IGs identified the following two problems:

- Continuous monitoring procedures were not fully developed, sufficiently detailed, or consistently implemented;
- Ongoing assessments of selected security controls had not been performed.

Multiple IGs also reported significant weaknesses in the following areas:

- Providing key security documentation to the system authorizing official or other key system officials;
- Strategy or plan had not been fully developed for entity-wide continuous monitoring;
- Continuous monitoring policy was not fully developed.

Contingency planning: FISMA requires agencies to plan and prepare for events that may impact the availability of an information resource. This process entails identification of important agency resources, potential risks to those resources, and the development of plans 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 is key to sufficient and cost-effective contingency planning. Critical systems may require multiple, redundant sites that run 24 hours a day, seven days a week, while less critical systems may not be restored at all after an incident. Contingency planning is essential for making these types of decisions 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 their agencies had contingency planning programs in place, but only eight IGs identified their agencies' contingency planning programs as fully consistent with applicable standards. The following three issues were prevalent among the 16 agencies needing improvements:

- Contingency planning procedures were not fully developed, sufficiently detailed, or consistently implemented;
- System contingency plans were missing or incomplete;
- Critical systems contingency plans were not tested.

Oversight of contractor systems: Contractors or other external entities own or operate many information systems on behalf of the Federal government, and these systems must meet the security requirements imposed on all systems that process or store Federal government information. As a result, these systems require additional oversight by the agencies that own or use them to ensure that they meet all applicable requirements.

Oversight of contractor systems is an area of significant concern across the Federal government. Only six IGs reported that their agencies were fully compliant with applicable requirements. Two agencies lack programs for overseeing contractor systems, while the remaining 16 IGs indicated that their agencies' programs need significant improvement. The most common weaknesses reported were:

- Procedures to oversee systems operated on the agency's behalf by contractors or other entities were not fully developed, sufficiently detailed, or consistently implemented;
- Systems owned or operated by contractors and entities did not meet NIST and OMB's FISMA requirements;
- Agency inventories did not identify interfaces between contractor/entity-operated systems to agency owned and operated systems.

Appendix 2. NIST Performance in 2010

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 of 2002 (FISMA), included duties and responsibilities for the National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Division (CSD). In 2010, CSD addressed its assignments through the following projects and activities:

- Issued 15 final NIST Special Publications (SP) that addressed management, operational and technical security guidance in areas such as securing WiMax wireless networks, secure content automation protocols, protection of personally identifiable information, Bluetooth security, and deployment of Secure Domain Name System deployment. In addition, eight draft SPs were issued for public comment for cryptographic key deployment and security configuration management among other topics.
- 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 consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls) for Federal information systems.
- Provided assistance to agencies and 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.
- As part of its contribution to the Smart Grid initiative, CSD released NIST IR 7628, *Guidelines for Smart Grid Cyber Security*, in August 2010.
- Reviewed security policies and technologies from the private sector and national security systems for potential Federal agency use. As part of this review, 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.
- Co-hosted the third annual HIPAA Security Rule conference, "Safeguarding Health Information: Building Assurance through HIPAA Security", to assist organizations in addressing security and privacy concerns in the growing use of HIT, and to discuss challenges, tips, and techniques for implementing the requirements of the HIPAA Security Rule.

- Developed conformance test procedures to ensure compliance with the HIT meaningful use security standards and certification criteria.
- Solicited recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines and solicited recommendations of the Board on information security and privacy issues regularly at quarterly meetings.
- Held a successful "SHA-3 conference" and selected five "finalist" candidate algorithms as a part of a public competition to select a new Federal cryptograph hash function standard.
- 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.
- Produced an annual report as a NIST Interagency Report (IR). The 2003-2009 Annual Reports are available via our Computer Security Resource Center (CSRC) website at http://csrc.nist.gov/ or upon request.

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