OFFICE OF
MANAGEMENT AND BUDGET

Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002

Table of Contents

Introduction: Current State of Cybersecurity

Our Nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. As stated in *The Cyberspace Policy Review*, the 60-day clean slate look at cyber activities ordered by the President, threats to cyberspace pose some of the most serious economic and national security challenges of the 21st century for the United States. The group of State and non-state actors who target U.S. citizens, businesses, and Federal agencies is growing. US-CERT, the computer response center for civilian agencies, sees millions of attempts daily to access open ports and vulnerable applications on Federal networks.

Historically, the Federal Government has not been as effective as necessary in its cyber defense. An inadequate cybersecurity workforce, a focus on compliance rather than outcomes, and a cumbersome and time-consuming process for collecting information regarding agency security postures have hindered our cybersecurity management capabilities.

In the seven years it has been in place, the Federal Information Security Management Act (FISMA), Public Law 107-347, has raised the level of awareness of the critical importance of information security in the agencies and in the country at large. It has also strengthened agency reporting requirements and established mechanisms for the collection of agency information. For example, based on agency FISMA submissions, security awareness training has become prevalent across the Federal Government for employees and contractors. Agencies and departments are now reporting inventory numbers for their systems, and CIOs play a critical role in managing information security in the agencies. However, continued progress must be made to realize FISMA's full vision of a secure and vigilant Federal Government.

When FISMA was first enacted, OMB approached the question of metrics by concentrating on compliance. During the first few years of FISMA reporting, the required metrics evolved as initial benchmarks were met.

These metrics were lagging indicators focused on compliance rather than outcomes. Agencies reported infrequently and, in many cases, only annually. This occurred in an environment where threat vectors change daily. Moreover, the information collected does not reflect the readiness of the agencies to deal with the reality of modern threats. Even information as basic as the cost of compliance or the number of days to apply a critical patch is not readily available.

OMB is committed to working across the Federal Government to address the important information technology security issues. On December 22, 2009, the White House announced the President's new White House Cybersecurity Coordinator, Howard Schmidt. As Coordinator, Schmidt will oversee Federal-wide coordination of the President's cybersecurity agenda, while working in tandem with the private sector on cybersecurity. OMB will also work with Coordinator Schmidt on these critical issues going forward.

The economic prosperity of our Nation relies upon, and is powered by, the digital infrastructure. Yet, security in the Federal Government is not where it needs to be. The Nation's approach to cybersecurity over the past 15 years has failed to keep pace with mounting threats. We are taking actions to improve the situation but are only at the beginning of what needs to be done. The Federal Government must remain committed to protecting the digital infrastructure upon which we so heavily depend.

I. 2009 Progress in Cybersecurity

A. Implementation of CyberScope

Prior to the 2009 FISMA reporting cycle, OMB received via email over 100 individual spreadsheets from agencies and paper copies of the Inspector General reports in response to FISMA reporting requirements. This manual spreadsheet process was laborious, time consuming, and transmission to OMB from agencies by email across the internet was unsecure. Furthermore, the lack of meaningful analysis, the vulnerable reporting methodology, and the manual nature of the process inhibited clear, timely, and comprehensive insight into the security posture of the Federal Government's information technology systems.

On October 19, 2009, OMB launched an interactive data collection tool—CyberScope—enabling agencies to fulfill their FISMA reporting requirements through a modern digital platform. The broad range of meaningful information collected, the use of secure two-factor authentication using Personal Identity Verification (PIV) cards, and the online access to data provides for a more efficient and effective reporting process.

Rather than relying on unencrypted emails sent across the Internet and unprotected spreadsheets, CyberScope requires users to login via a PIV card and an accompanying unique PIN number. The PIV card was mandated for use by all Federal employees by the Homeland Security Presidential Directive 12 (HSPD-12).

CyberScope empowers its 600 estimated users to manage their internal reporting and information collection processes as best suits their individual needs. OMB conducted training sessions prior to the launch of CyberScope and utilized much of the feedback to improve the system. Going forward, CyberScope's extensible platform is the performance-based solution to years of inefficient and unsecure collection of agency security data.

B. Development of New Information Security Performance Metrics for 2010

What gets measured gets done; metrics are policy statements. As long as OMB metrics continue to measure compliance, agencies and departments will continue to march toward that goal. However, we can never get to security through compliance alone.

In September 2009, OMB established a task force to develop new, outcome-focused metrics for information security performance for Federal agencies. To solicit the best ideas, OMB reached across the Federal community, as well as to the private sector. This task force concentrated on developing metrics that will advance the security posture of agencies and departments. Understanding that metrics are a policy statement about what Federal entities should concentrate resources on, the task force developed metrics that will push agencies to examine their risks and make substantial improvements in their security.

Participants in the task force included: the Federal CIO Council, which includes the CIOs of civilian agencies, 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.

The task force developed forward-looking metrics focused on improving security at agencies rather than merely demonstrating compliance. Additionally, the task force is working with OMB to develop a roadmap for future reporting under FISMA which will incorporate real-time metrics and enhance government-wide situational awareness.

OMB released the FY2010 metrics for public comment in November 2009. OMB plans to release the final metrics and reporting instructions for future reporting efforts in the spring of 2010. As with past years, in 2010, agencies will report on performance-oriented metrics in the fall.

C. Collection of Information Security Costs

This reporting cycle, for the first time, OMB asked agencies for detailed cost estimates and the actual amounts spent on information security. Historically, as part of the annual budget process, agencies reported only the percentage of spending related to cybersecurity for each IT investment. However, this information was not broken down into distinct categories, such as personnel costs, reporting costs, certification and accreditation (C&A) costs, and security management costs. This lack of detailed information precluded the level of meaningful analysis needed to assess the efficiency and effectiveness of Federal information security spending.

Recognizing that the best security is "baked in" to information technology investments and not added in separately, OMB needs to determine where in the life cycle development of systems agencies are spending their resources. The information collected for FY 2009 is the beginning of the process of obtaining this crucial cost data.

In the coming years, access to continually refined cost data will allow OMB to evaluate the efficiency of the Federal expenditure on security. Right now, the Federal Government cannot answer key questions such as: “Is the Federal government spending too much on certification and accreditation, considering its benefits?” The collection of detailed information, especially when combined with performance-based metrics, will allow both OMB and agency management to make informed, risk-based decisions on where to allocate scarce resources.

D. Information Systems Security Line of Business (ISSLOB) Progress in 2009

The Information Systems Security Line of Business (ISSLOB) is an interagency effort managed on behalf of OMB by the Department of Homeland Security (DHS). Implemented in 2006, the ISSLOB identifies common information security needs across the Federal Government and delivers product and service solutions to improve information security program performance, reduce costs, and increase efficiency across the federal enterprise.

The ISSLOB delivers these solutions through the establishment of government Shared Service Centers (SSCs) and also partners with the General Services Administration (GSA) to deliver strategic government-wide acquisition vehicles.

In FY 2009, ISSLOB continued to support the original Shared Service Centers (SSCs) for FISMA Reporting, and General Security Awareness Training, through information sharing and customer agency outreach. Additionally, the ISSLOB established four new SSCs in late FY 2009 that will provide federal agencies with a service provider option for managed Certification and Accreditation (C&A) services. A Customer Advisory Board (comprised of members of the Federal IT security workforce) was also established to provide more coordination and oversight guidance to existing the SSCs and their customers.

The ISSLOB and GSA SmartBuy announced the award of the Situational Awareness and Incident Response (SAIR) Tier I Blanket Purchase Agreements (BPAs) in the fourth quarter of FY 2009. Through collaborative efforts involving agency stakeholders across the government, the ISSLOB identified tool sets that will fulfill key capability gaps in conducting vulnerability assessments, network mapping and discovery, and baseline configuration management activities. These tools can help agencies develop an accurate inventory of information resources managed at their agency, and maintain an up-to-date awareness of information regarding cybersecurity threats. Federal agencies have begun to utilize the BPAs to procure products associated with this acquisition. Agencies utilizing the SAIR Tier I SmartBUY BPAs have realized cost savings of 20% versus standard GSA pricing (IT schedule 70). In addition, these BPAs are also accessible to state and local governments, allowing them to leverage federal acquisition efficiency.

The ISSLOB will continue to work with its acquisition and federal civilian agency partners to Award BPAs for SAIR Tier II and Industry provided C&A Services. The ISSLOB will continue to engage their cross-government stakeholders and the Federal Systems Security Governance Board (FSSGB) to identify other opportunities, such as DNSSEC implementation, where commercial products and managed services may assist agencies in their implementation efforts of policy mandates and Info Sec initiatives.

The ISSLOB will strive to increase cost savings for Federal civilian agencies as more SSCs are established, and will work with its SSC partners and the ISSLOB Customer Advisory Board (comprised of members of the Federal IT security workforce) to ensure that subject matter and service level requirements are refreshed appropriately. This will ensure that existing and new customers' missions are adequately supported through their utilization of the SSCs.

In order to provide a more cost effective approach, the ISSLOB is planning to enhance its General Security Awareness Training (Tier I) SSC offerings through a centrally managed subject matter expert review of the Tier I SSC training materials. The SSC content will be examined to ensure consistencies in scope, sequencing, outcomes, and performance expectations associated with completion of the course content across all Tier I Training SSCs.

E. Information Security Workforce

As the Department of Homeland Security (DHS) grows into its role of protecting the homeland in cyberspace, it must have a skilled workforce capable of securing networks, understanding the threats we face, and assisting Federal agencies in defending their networks. Recently, OMB worked closely with the Office of Personnel Management (OPM) to extend special hiring authority to DHS to meet its growing needs.

On October 1, 2009, DHS Secretary Janet Napolitano announced that DHS has the authority to hire up to 1,000 new cybersecurity professionals over the next three years to fill staffing gaps at various DHS agencies. DHS will look to fill critical cybersecurity roles including: cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering. This new hiring authority will enable DHS to recruit skilled cyber analysts, developers, and engineers to serve their country by helping to secure the nation against cyber threats.

II. Incidents and Response in the Federal Government

The Federal Government faced two major incidents in 2009, the Conficker worm and the July 4th distributed denial of service (DDOS) attacks. These were two distinct types of incidents and required different responses. Yet they both pointed to the need to improve federal response capacity.

The Conficker worm (also known as Downadup) began circulating in November 2008. It utilized multiple attack vectors to compromise vulnerable systems, including previously patched vulnerabilities. In addition, there were several variants of the worm circulating, with the later variants deploying a number of countermeasures to preclude detection by security applications and block legitimate system updates. At this point, Conficker is one of the most common infections on the internet. It is estimated that over 1.7 million machines are currently infected.[1]

The Federal Government response began in January 2003, when US CERT released its first notices to the agencies concerning the spread of the worm. US CERT also joined the Conficker Working Group, a public-private partnership. In March 2009, in anticipation of a malicious payload in the C variant of the worm, agencies were asked to take immediate action to determine levels of infections in their infrastructures and to take corrective actions.

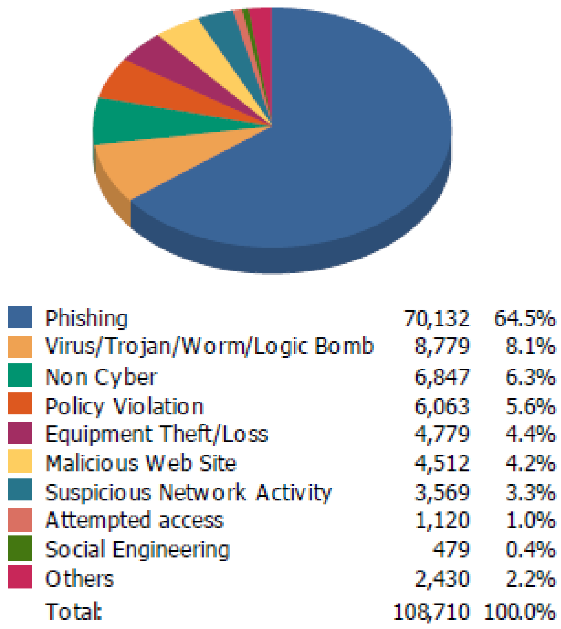
The DDOS attacks began on the July Fourth weekend in 2009. A large botnet (a network of infected machines, operated remotely) began attacks on a wide range of private, public and governmental websites. Some federal agencies did experience denial of access to websites. US CERT coordinated the response to attacks for the federal governments. They worked with both federal agencies and the information service providers used by the agencies to mitigate the attacks.

There were several lessons learned from these two attacks about the readiness and responsiveness of federal agencies and departments:

- Communications – reaching out across an entity the size of the Federal Government, even a portion, such as the Civil Executive Branch, is a daunting task. Information did not always reach the right people at the agency so that effective actions could be taken timely.
- Capabilities – departments and agencies did not have the capability to easily or quickly to review their infrastructure for relevant vulnerabilities or infection status.
- Outdated assumptions – the traditional response methods did not work for the attacks.

[1] Team Cymru Research NFP, http://www.team-cymru.org/Monitoring/Malevolence/conficker.html

Top Incidents and Events in the Federal Network



Source: US-CERT, 2009.

These lessons learned are informing federal activities in cybersecurity. The need for better communications and more capabilities were included as considerations for the development of the new metrics for 2010 FISMA reporting. The Department of Homeland Security, in consultation with the Information Security and Identity Management Committee of the Federal CIO Council, is working on developing new incident taxonomies and response plans.

III. Analysis of Key Security Metrics

Overall, agencies continued to report increases in compliance with the requirements of FISMA in FY 2009. Percentage of systems with current certifications and accreditations remained high at 95%. In addition, agencies are training their work force in basic security awareness at high levels, and are reporting their incidents on a regular basis to the proper authorities. Information on agency reporting measures can be found in Appendix I.

A. Information Security Cost Information

Availability of resources can have a major impact on the cybersecurity posture of an agency. In the past, OMB collected very little detailed cost data on cybersecurity spending of the federal agencies. For example, agencies were required by *Circular A-11* to identify for each IT investment what percentage of overall cost was applicable to cybersecurity, and they were asked for the amount they spend on cybersecurity training each year. This does not give OMB much visibility into the spending of the agencies, nor does it allow us to understand and assist the agencies in directing spending towards activities that benefit the cybersecurity posture of the Federal government.

During the FY 2009 FISMA data collection, OMB asked a number of detailed cost questions on cybersecurity:

- Provide the amount that the Agency has spent on certification and accreditation activities in FY 2009. Include all aspects of C&A activities including: risk assessments, security plan preparation, security testing, etc. (This amount should not include staff costs also known as full-time equivalents or FTEs)
- How many systems underwent certification and accreditation (either new systems, or as part of the 3 year cycle or major modification) in FY 2009 at your Agency?
- Provide the amount that the Agency has spent on periodic security testing in FY 2009 (other than testing performed as part of certification and accreditation activities). (This amount should not include FTEs)
- Provide the number of government FTEs whose duties are primarily security-related at your Agency in FY 2009.
- Provide the number of contractor FTEs whose duties are primarily security-related at your Agency in FY 2009.

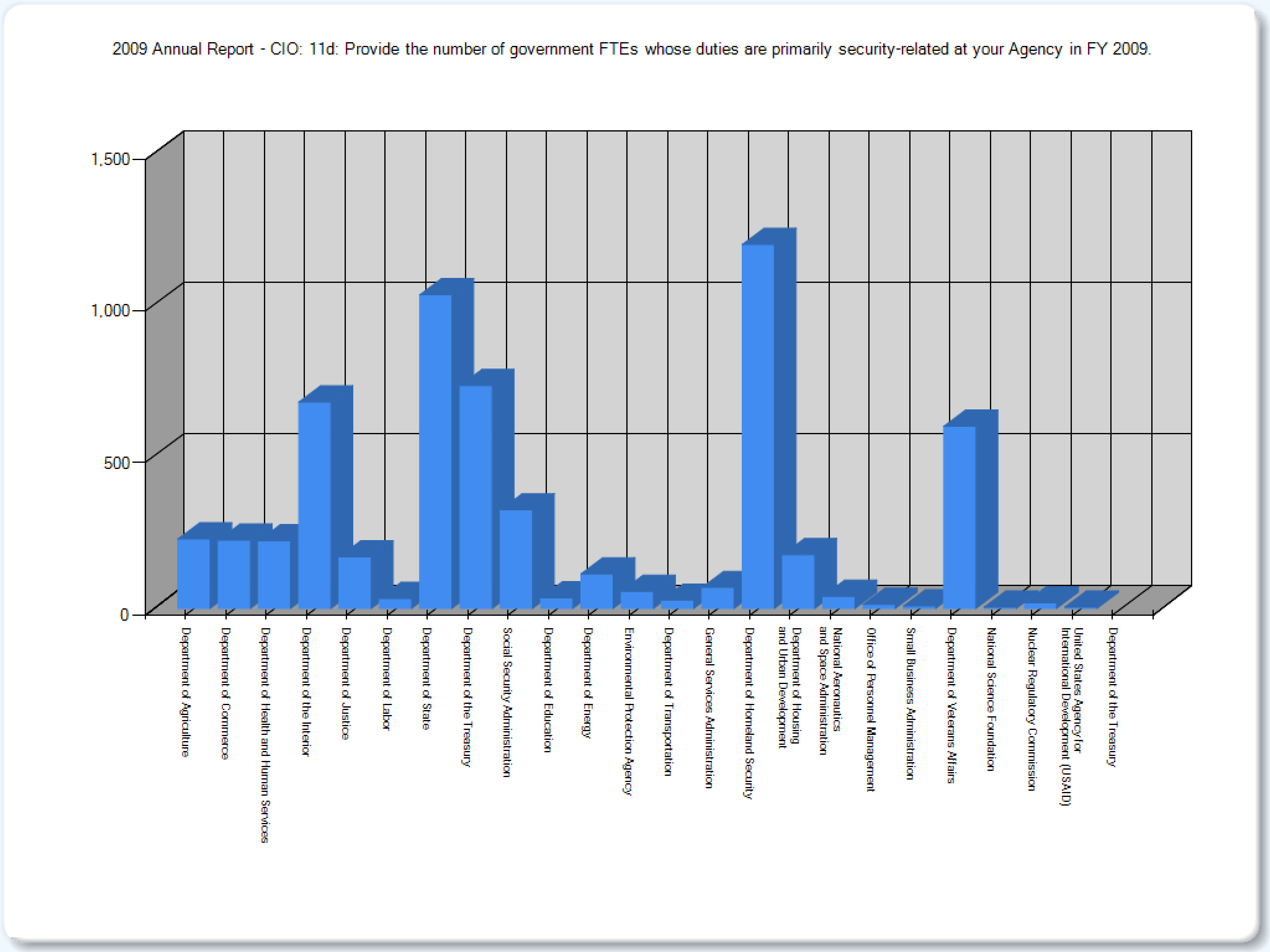
Since OMB has never asked for detailed cost data for cybersecurity activities, many agencies were not tracking costs in the categories asked for. Therefore, costs in some cases may be estimates rather than actual spending. This is especially true for agencies that use multi-function contracts for security (i.e., the contract is for multiple security activities). OMB anticipates that detailed cost data for agencies will become more accurate in future years. Numbers of FTEs and systems undergoing certification and accreditation were tracked and agencies were easily able to furnish these data.

The single largest cost driver in cybersecurity in the Federal Government, according to the data reported by the agencies, is costs for government employees. Agencies reported over 60,000 Full Time Equivalent (FTE) positions with primarily security-related duties. At an average cost of $159,000 per FTE, the cost for these employees exceeds $10 billion.[2] Already, this information provides more visibility into Federal cybersecurity spending then was previously available. The total estimated dollars for cybersecurity reported by the agencies for the 2009 President's Budget[3] was approximately $6.8 billion. So, actual FTE costs then equal 150% of the amount that agencies anticipated spending in the 2009 budget.

[2] This number includes both salary and benefits as defined in OMB Circular A-11.

[3] The costs reported were the actual for FY 2009 and thus are compared to the data reported as part of the FY 2009 President's Budget.

The majority of FTEs with security related responsibilities were reported at the Department of Defense, which is also the largest employer in the Federal Government. As can be seen in the graphic below, the Department of Homeland Security reported the second largest number of FTEs with the Department of State reporting the third largest amount.



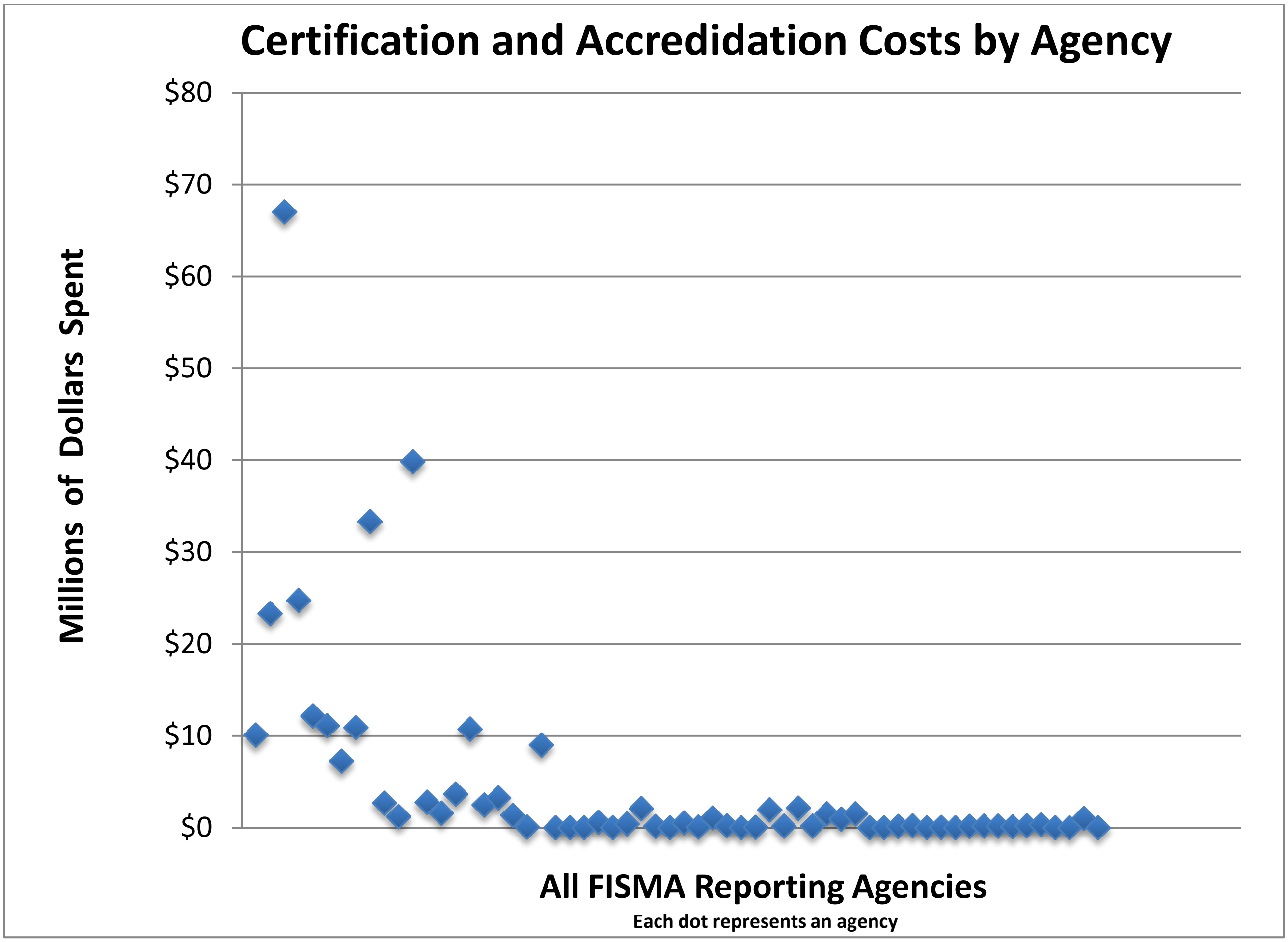
In addition to government employees, agencies reported that they had more than 30,000 contractors working on security-related activities in 2009.

The Department of Defense reported the highest amount of contractor FTEs, followed by the Departments of State and Homeland Security.

Certification and Accreditation Costs—Certification and accreditation is the process by which Federal agencies are required to apply a process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. This process applies to all agency-owned or contractor systems operated on behalf of a federal agency. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision. The security certification and accreditation process consists of four distinct phases:

- Initiation Phase;
- Security Certification Phase;
- Security Accreditation Phase; and
- Continuous Monitoring Phase.

Certification and accreditation have been cited by some sources as a major drain on agencies' cybersecurity resources. To determine the extent of the issue, we asked the agencies to provide us with the costs associated with these activities for FY 2009. Agencies varied widely in the costs that they reported.

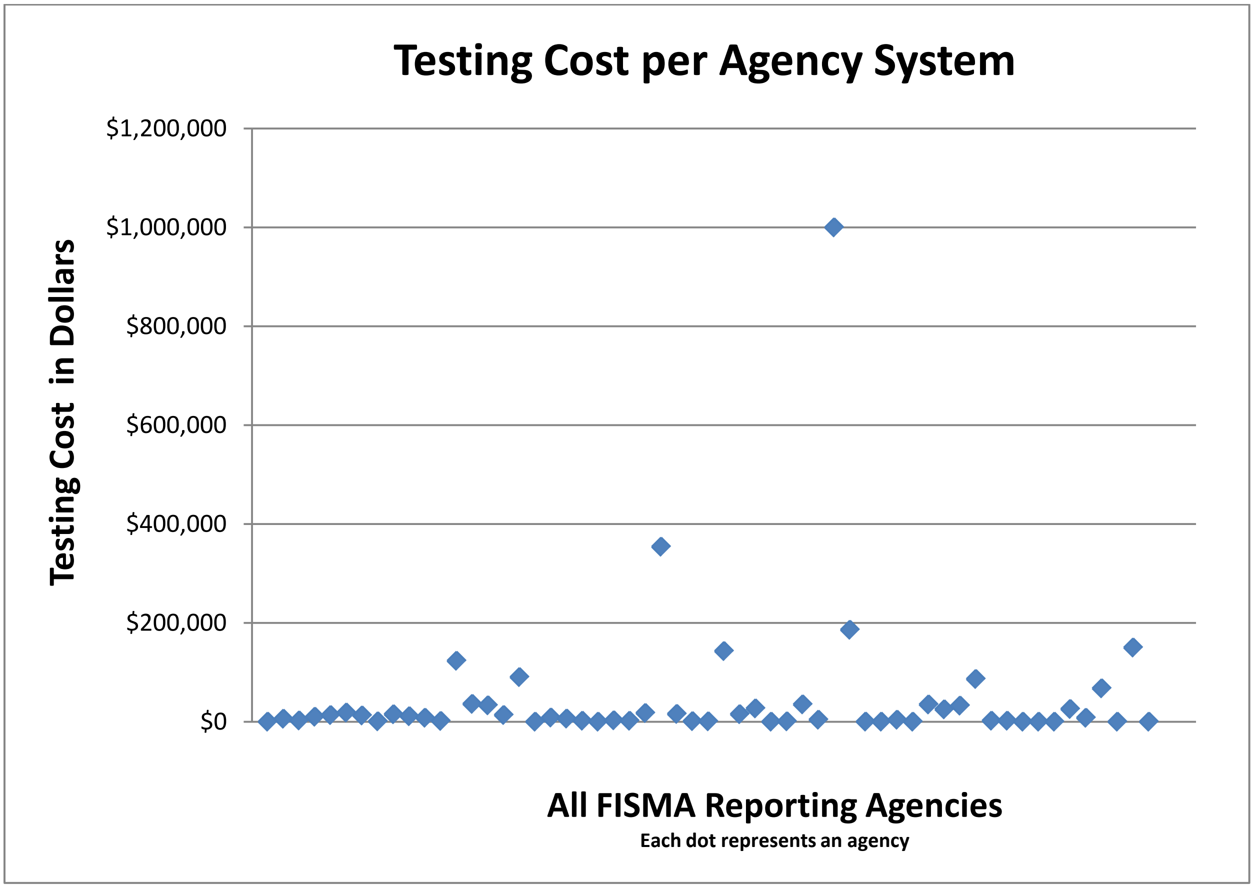


Overall, agencies reported spending almost $300 million in certification and accreditation activities. This amount is about 4% of the $6.8 billion reported for all cybersecurity activities for the FY 2009 President's Budget.

OMB also asked agencies to provide us with the number of systems that agencies had conducted certification and accreditations on within the year. OMB used this information to calculate an average cost per agency per system and an average cost per system for the entire federal government. While the average cost across the federal government was about $78,000, the average per system at the agencies varied widely.

Costs of certification and accreditation activities are based on a variety of factors. For example, the complexity of the system (number of servers, multiple locations, etc.) may mean that a system will cost more to certify and accredit. In addition, the risk categorization of the system directly impacts the cost of certification and accreditation activities. High and medium risk systems have more system controls and require more extensive testing. Even the number of systems may impact cost; if an agency has multiple similar systems, they may be able to achieve cost efficiency for coverage of all systems. The highest average cost was not at the 25 largest agencies, although several of them reported higher than average costs per system.

Annual Testing—FISMA requires that agencies test the operational, managerial and technical security controls on their systems at least annually. OMB asked agencies to report the cost of these testing activities, excluding the government FTE costs and the testing done during the certification and accreditation process. Agencies reported that they spent about $165 million on security testing. This amount represents 2% of the reported $6.8 billion for security costs that agencies reported for the FY 2009 President's Budget. This also represents an average cost per system of $21,000. Again, testing cost per system varied widely across the Federal Government. Testing costs may vary for a variety of reasons. Agencies may test more often then annually, especially with systems that are categorized as high risk. Again, system complexity will also impact testing costs. An agency with a few large, complex systems may have a much higher average testing cost than an agency with more systems, but ones that are less complex. Finally, the rigor of the testing will impact costs. Agencies design testing on a risk-benefit cost model.



B. The Responses of the Inspectors General

The Inspectors General are asked about several aspects of the agencies' security management program. They are asked questions designed to elicit information about the effectiveness of the security management program at the agencies. The areas include:

- certification and accreditation
- management of contractors
- inventory management
- the remediation for known security weaknesses process

Overall, the IGs reviewed approximately 9% of federal systems (including both agency and contractor owned systems). For the 24 large agencies, the IGs reviewed an average of 6% of agency-operated systems and 14% of contractor owned systems. Twenty-two IGs reviewed all the systems their agencies had in their FISMA inventory; this included three of the large agencies.

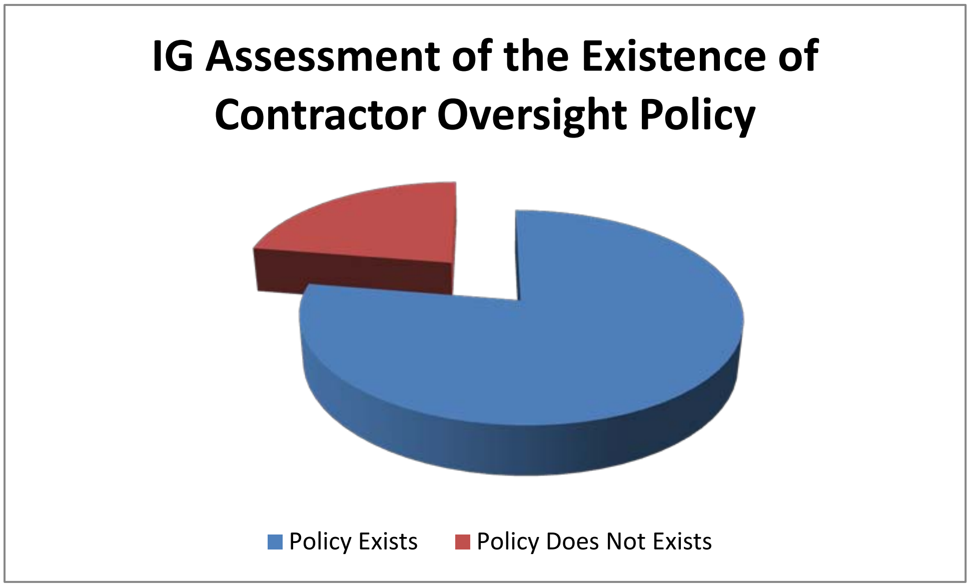
Certification and Accreditation—The Inspectors General were specifically asked about the different components of the certification and accreditation program as well as about the overall program.

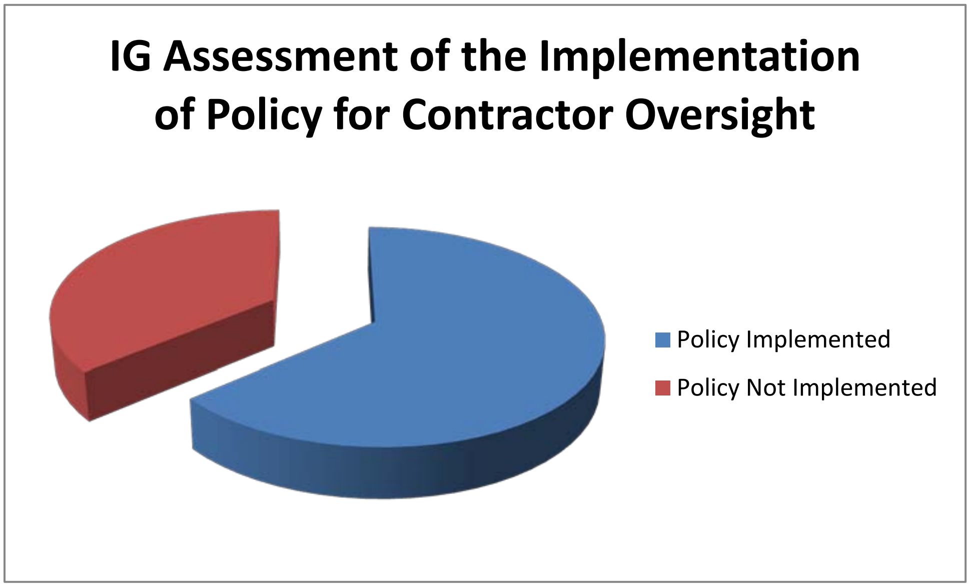
Overall, according to the IGs, 90% of the agencies have certification and accreditation policies in place that were compliance with requirements and guidance. However, the IGs identified only 67% of agencies as following correctly managing and operating their certification and accreditation programs in accordance with agency policy. Therefore, according to the IGs, almost one-third of agencies are not managing the certification and accreditation process in line with their policies or in accordance with requirements and guidance.

IGs assessed the majority of the agencies as having certifications and accreditation programs that were implemented and managed in compliance with requirements and guidance. However, the IGs did identify concerns with testing in almost a third of agencies. The IGs identified that just under a quarter of agencies had concerns with risk categorization, both assigning the category and the assessments.

Contractor Oversight—Proper management and oversight of contractors, both those operating contractor-operated FISMA systems, and those working on agency-operated systems, is essential for agencies if they are to secure their systems. Agencies reported over 30,000 contractor FTEs and this may not include contractors who are working on contractor-operated systems and are not issued agency credentials. Agencies are required to have FISMA controls over their contractor-operated systems. To standardize these requirements, the Federal Acquisition Regulations (FAR) has several clauses that should be included in contracts to facilitate and the agency should have policies and procedures around contractor oversight.

IGs were asked if their agencies had policies in accordance with applicable guidance and requirements for the oversight of contractors. They were also asked if the agencies had implemented the policies and procedures. While 78% of the IGs agreed that their agencies had policies for the oversight of contractors, only 64% agreed that their agency had implemented those policies.





Inventory Management—FISMA requires that agencies maintain an up-to-date inventory of their information systems, including both agency and contractor-operated. The IGs were asked a series of questions about the existence, maintenance and accuracy of agencies' inventories:

- Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?

- Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?
- Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?
- The Agency inventory is maintained and updated at least annually.
- The IG generally agrees with the CIO on the number of Agency-owned systems.
- The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency.

Overall, IGs (93%) agreed that their agencies had materially correct inventories that were maintained on at least an annual basis. More IGs agreed with their agencies about the correctness of the inventory of the agency-operated systems then with the accuracy of the contractor-operated systems..

Interfaces are electronic connections between the agency’s network and another entity’s network. Because of the risks associated with extending permanent access to your network to another entity, agencies should, according to NIST guidance, takes steps to assure themselves of the security of the connections. In order to gain some assurance, the agencies should enter into formal agreements with the other entity. These agreements spell out the security responsibilities of each party. Agencies should maintain an inventory of such interfaces and require that all interfaces have agreements.

Just under three-quarters of all agencies maintain inventories of their interconnections, according to the IGs. If agencies do not maintain an inventory and update it, it is possible that there are interconnections that the agency may be unaware of. These connections can pose serious security risks as they constitute a connection directly into the agency’s system. Moreover, according to the IGs, only 88% of agencies had policies requiring interconnection agreements to be in place.

Remediation for Known Weaknesses (Plans of Actions and Milestones)—FISMA requires that agencies develop and maintain remediation programs to mitigate risks caused by identified security vulnerabilities. These remediation programs are generally referred as plans of actions and milestones (POA&Ms). The IGs are asked to evaluate agency management of the POA&M process. Specifically, they were asked:

- Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?
- Has the Agency fully implemented the policy?
- Is the Agency currently managing and operating a POA&M process?
- Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weakness, including IG/external audit findings associated with information

systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency?

- Does the POA&M process prioritize IT security weakness to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?
- When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?
- Are deficiencies tracked and remediated in a timely manner?
- Are the remediation plans effective for correcting the security weakness?
- Are the estimated dates for remediation reasonable and adhered to?
- Do Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?
- Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?

Although, overall, the IGs for almost ¾ of the agencies reported that their agencies had a good POA&M process, almost half of the IGs reported concerns with actual remediation processes. For example, IGs reported that only 55% of the agencies tracked and remediated weaknesses in a timely manner. Many of the concerns the IGs raised may cause a delay in the remediation of an identified vulnerability. For example, IGs reported such concerns as resources may not be available or the plan may lack a technical answer to remediate the vulnerability. The majority of the IGs did report that remediation plans were effective. However, less than half of the agencies meet the dates of the milestones in their plans according to the IGs.

C. Training

During the FY 2009 FISMA data collection, OMB continued asking agencies the following questions on training:

- What is the total number of people with log in privileges to Agency systems?

- What is the number of people with log in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, “Building an Information Technology Security Awareness and Training Program”?

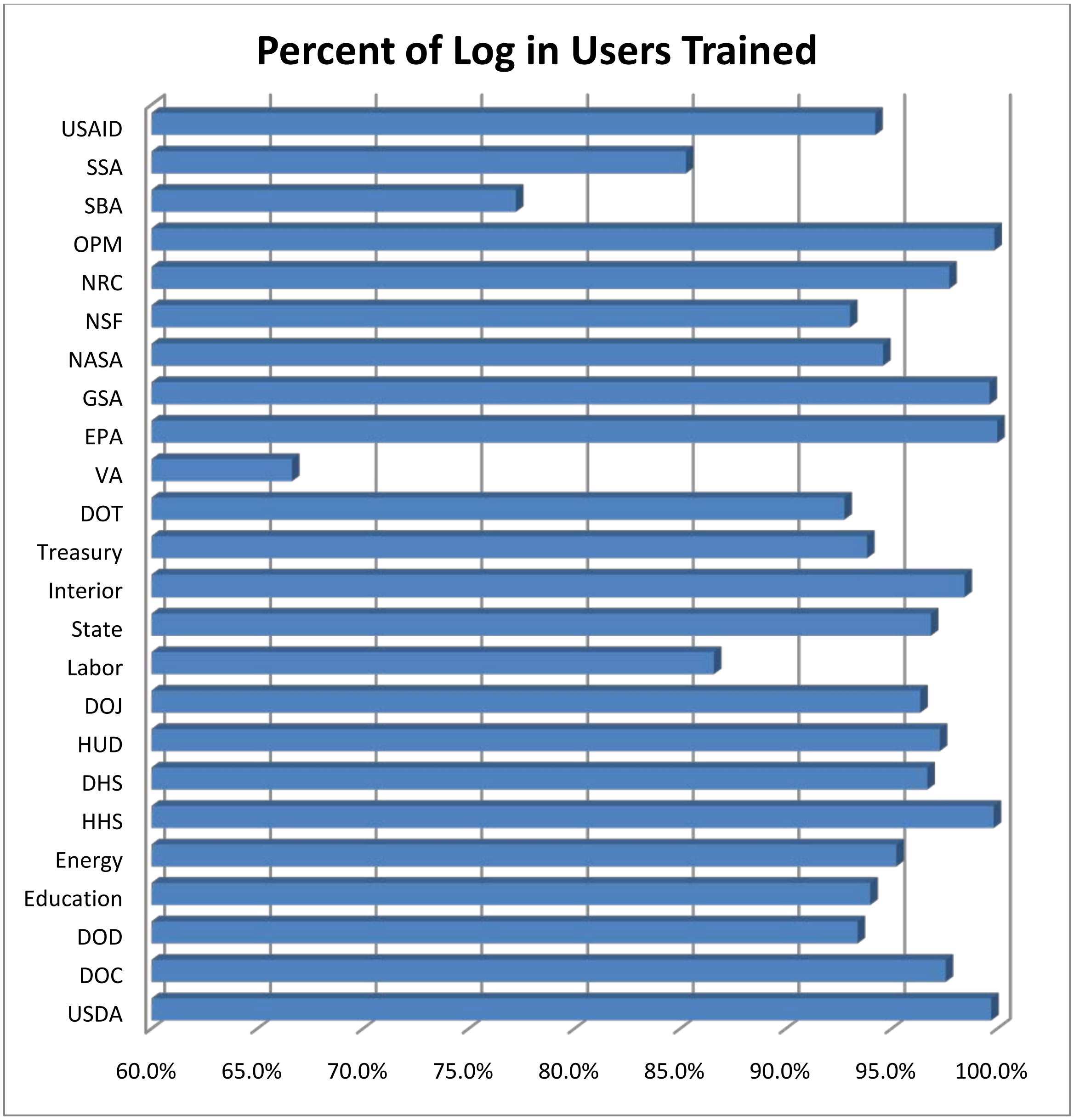
- What is the number of people with log in privileges to Agency systems that received information security awareness training using an ISSLOB shared service center?

- What is the total number of employees with significant information security responsibilities?

- What is the number of employees with significant responsibilities that received specialized training as described in NIST Special Publication 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model”?

- What were the total costs for providing information security training in the past fiscal year?

Agencies reported that 91% of individuals with log in privileges to Agency systems received information security awareness training during the past fiscal year. Of those trained, 57% were trained using an ISSLOB shared service center. In FY 2009, 90% of employees with significant information security responsibilities received training. The security training of all of these individuals cost agencies $52.4 million dollars in FY 2009 alone. However, due to the risk of double counting individuals who had both log in privileges and significant information security privileges, OMB is unable to determine the exact cost per individual of security training for the fiscal year. All 24 major agencies reported that their agency’s information security awareness training, ethics training, or any other Agency-wide training covered the use of peer-to-peer file sharing.



Four of the 24 major agencies' IGs reported that these agencies had not developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log in privileges and provide those individuals with suitable IT security awareness training. Only one agency's IG determined that their agency's information security awareness training, ethics training, or any other Agency-wide training covered the use of peer-to-peer file sharing.

IV. Progress in Meeting Key Privacy Performance Measures

As discussed in the sections that follow, the FY 2009 agency FISMA reports indicate general improvements in many privacy performance measures, although additional work is needed in areas such as agency PIA processes and compliance.

Status and Progress of Key Privacy Performance Measures

	FY 2007	**FY 2008**	**FY 2009**
Number of systems containing information in identifiable form	3,259	3,505	4,266
Number of systems requiring a PIA	1,826	2,002	2,605
Number of systems with a PIA	1,525	1,850	2,319
Percentage of systems with a PIA	**84%**	**92%**	**89%**
Number of systems requiring a SORN	2,607	2,373	3,373
Number of systems with a SORN	2,169	2,205	3,243
Percentage of systems with a SORN	**83%**	**93%**	**96%**

Privacy Program Oversight

In 2009, 24 out of 25 senior agency officials for privacy (SAOP) 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, 24 out of 25 agencies reported having policies in place to ensure that all personnel with access to Federal data are familiar with information privacy requirements, and 23 out of 25 agencies reported having targeted, job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 100 percent of applicable systems to have publicly posted PIAs. In 2009, 89 percent of applicable systems across the 25 major agencies had publicly posted PIAs, a decrease from 92 percent in 2008. The decrease occurred as the number of systems requiring a PIA increased.

Quality of Privacy Impact Assessment Process

FISMA reporting guidance asks agency IGs to rate the quality of each agency's PIA process. In 2009, 23 out of 25 agency IGs reported that their agency has developed and documented an adequate policy for PIAs. However, the IGs of 14 of those 23 agencies with adequate PIA policies reported that their agency has fully implemented the policy and is managing and operating a process for performing adequate PIAs.

System of Records Notices

The Federal goal is for 100 percent of applicable information systems with Privacy Act records to have developed, published, and maintained SORNs. In 2009, 96 percent of information systems government-wide with Privacy Act records have published current SORNs. The percentage represents an overall increase from 2008, despite a significant increase in the number of information systems required to be covered by a SORN.

Privacy-Related Policies and Plans

FISMA reporting guidance asks agency IGs to determine whether each agency has developed and documented adequate policies that comply with OMB guidance for safeguarding privacy-related information. In 2009, 17 out of 25 agency IGs reported that their agency has developed and documented adequate policies.

On May 22, 2007, OMB issued Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,*[4] setting forth four new privacy directives for agencies to:

- Develop and implement a breach notification plan;
- Implement a plan to eliminate unnecessary collection and use of SSNs in agency programs;
- Implement a plan to review and reduce unnecessary holdings of PII; and
- Develop policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

OMB requested up-to-date plans and policies associated with the requirements. Since the issuance of M-07-16, agencies demonstrated progress in establishing breach notification plans, providing a better foundation for responding to breaches of PII. Most agencies were able to provide formal, comprehensive breach notification polices. Agencies also included model documents, such as sample breach notification letters, along with the plans for rapid response to a breach.

Despite varying levels of detail and comprehensiveness across agencies, the submitted plans for reducing unnecessary Social Security Numbers (SSNs) and PII, as well as establishing related rules of behavior, generally demonstrate agency officials have been sensitized to the privacy risks associated with SSN and PII holdings. The efforts will require on-going oversight through the capital planning process, Paperwork Reduction Act reviews, Executive Order 12866 regulatory reviews, and other oversight mechanisms. In order to facilitate agency SSN reduction

[4] Which can be found at: http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf

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.

V. Path Forward

A. Implementation of New Information Security Performance Metrics

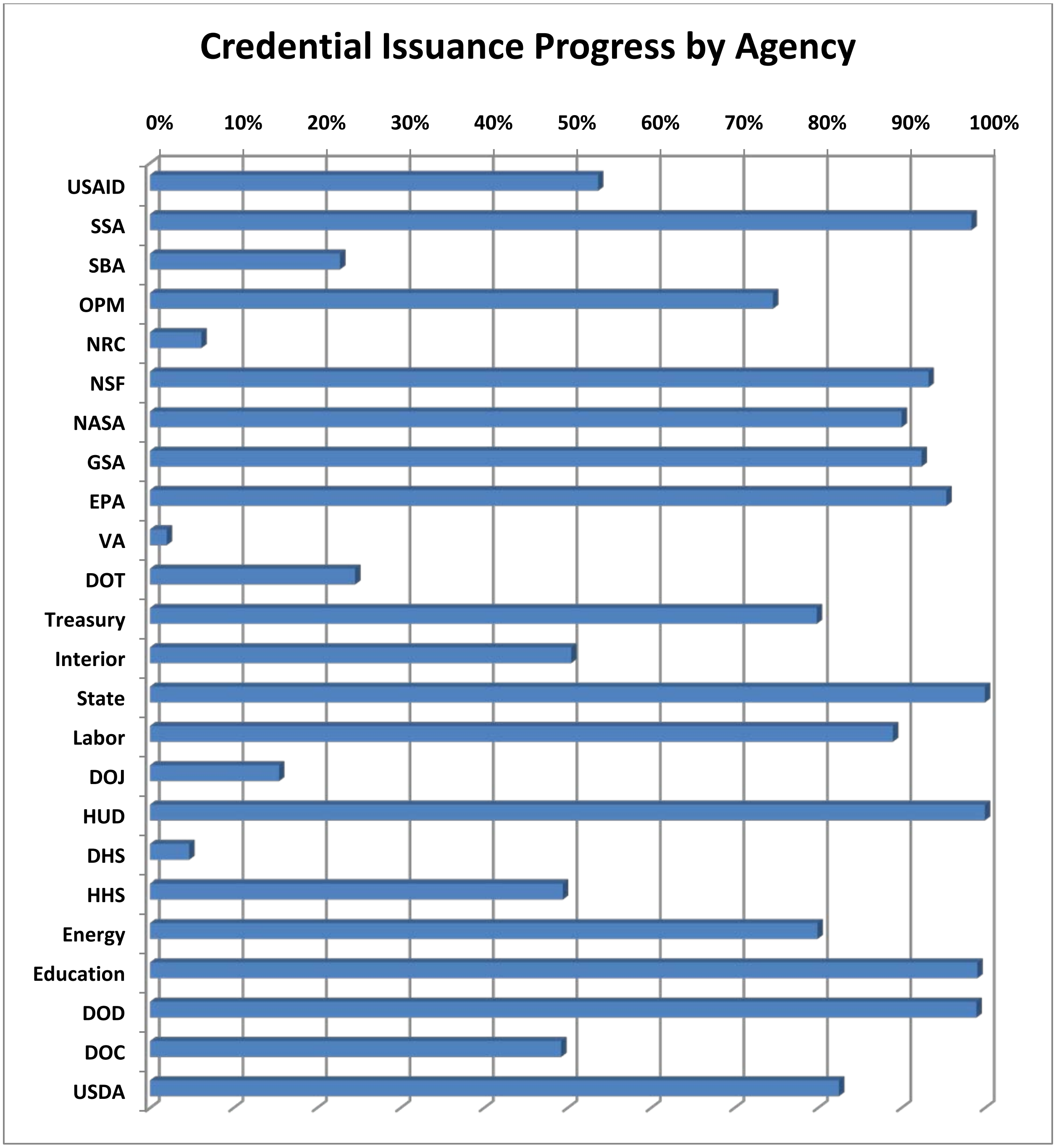
The new metrics developed by the Security Metrics Task Force will be used in agencies 2010 FISMA reports to OMB and the Congress. Additionally, OMB will release a roadmap for future reporting under FISMA, which will incorporate real-time metrics and enhance Government-wide situational awareness in 2010. With the FY 2010 metrics, near or at real-time frequency of reporting, OMB is taking its first move towards developing situational awareness across the Federal government. The use of Security Information Management or Security Information Event Management tools will assist in progressing towards real time security awareness and management in the Government.

B. Federal Identity Management

The Cyberspace Policy Review outlined a number of cybersecurity recommendations. To support this effort, the Federal Chief Information Officers’ Council developed the “Identity, Credential and Access Management (ICAM) Roadmap and Implementation Guidance” document to provide implementation guidance for program managers, leadership, and stakeholders as they plan and upgrade their architectures. One of the major outcomes of this effort is to enable agencies to create and maintain information systems that deliver more convenience, appropriate security, and privacy protection, with less effort and at a lower cost. The ICAM roadmap, issued in November 2009, outlines a number of transition activities for agencies to complete. It also serves as an important tool for providing awareness to external mission partners and driving the development and implementation of interoperable solutions. ICAM solutions will leverage the existing investments in the Federal Government while promoting efficient use of tax dollars when designing, deploying, and operating ICAM systems.

As part of this effort, OMB will continue to oversee the implementation of the strong Federal identity management scheme outlined in Homeland Security Presidential Directive 12 (HSPD-12). This directive, “Policy for a Common Identification Standard for Federal Employees and Contractors,” addressed the September 11th Commission recommendation to improve the security of Federal facilities and information systems. Agencies are required to follow specific technical standards and business processes for the issuance and routine use of Personal Identity Verification (PIV) smartcard credentials including a standardized background investigation to verify employees’ and contractors’ identities. When used in accordance with NIST guidelines, the credentials provide a number of benefits to 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, 2009, over 5 million PIV credentials (82 percent of those needed) were issued to the Federal workforce, as reported by agencies. With the majority of the Federal workforce now in possession of PIV credentials, agencies can focus on making the electronic capabilities of the credentials available to a broad user base. FISMA requires agencies to ensure that information security is addressed throughout the life cycle of each agency information system. By leveraging the capabilities of the PIV credentials, agencies can address long-standing FISMA requirements through the use of a common government-wide standard. To better monitor agency progress, the FISMA Metrics Task Force has developed new metrics for HSPD-12 that focus on the usage of the credentials for routine access to systems. The agency progress information will be presented in future FISMA reports.



C. Security Aspects of Administration Priorities

Open Government & Web 2.0—The Administration is committed to launching new, innovative platforms for increasing transparency, encouraging participatory government, and collaboration among and within Federal agencies. Recognizing that with increased collaboration and transparency, agencies face increased threats to IT security, the Administration is committed to including security measures in the initial implementation phases of social media tools, not tacking on important safeguards after the fact. OMB and OSTP, in partnership with GSA's Citizen Engagement Platform, will implement the secure use of new media outlets across the Federal Government.

Health Information Technology (HIT)—As the Federal Government implements the requirements of the HITECH Act of 2009, the Administration will continue to leverage Federal information technology to support goals for population health, encourage care coordination through the development of interoperability standards, and assist the development and integration of privacy and security protections into the HIT framework.

Cloud Computing—Adoption of a cloud computing model is a major part of the strategy to achieve efficient and effective IT. After evaluation in 2010, agencies will deploy cloud computing solutions across the Government to improve the delivery of IT services. There will be an online storefront to enable subscribers to access lightweight collaboration tools, software, and platform and infrastructure service offerings in a cloud environment. Cloud computing will be implemented in a secure manner.

Game Changing Technologies—Unclassified Federal cybersecurity research and development is coordinated through the Cybersecurity and Information Assurance (CSIA) Interagency Working Group. This group is a component of the Networking and Information Technology Research and Development Program of the NSTC's Committee on Technology.

R&D priority areas for the CSIA agencies range from fundamental investigation of scientific bases for hardware, software, and system security to applied research in security technologies and methods, approaches to cyber defense and attack mitigation, and infrastructure for realistic experiments and testing. Emphases include:

- Foundations: Cybersecurity as a multidisciplinary science;

- Applied and Information Infrastructure Security: Secure platforms and networks, trustworthy environments;

- Situational Awareness and Response: Attack detection, management, and attribution, assured operations in high threat environments, security management; and

- Infrastructure for R&D: Testbeds, ranges, tools, platforms, and repositories.

Appendix 1: Government-wide Data Summary Charts

Table 1: Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2009 for the 25 Major Agencies

Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Certification and Accreditation	47%	62%	77%	85%	88%	92%	96%	**95%**
Tested Contingency Plan	35%	48%	57%	61%	77%	86%	92%	**86%**
Tested Security Controls	60%	64%	76%	72%	88%	95%	93%	**90%**
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304	10,679	**12,930**

Table 2: Fiscal Year 2009 FISMA System Inventory by Risk Impact Level

FIPS-199 Level	High	Medium	Low	Not Categorized
Agency Systems	2315	8906	7925	527
Contractor Systems	303	1469	847	1567
Systems owned by another Federal Agency	118	315	138	79
Total Number of Systems (Agency and Contractor systems)	2618	10375	8772	2094
Number (and Percentage) of systems certified and accredited	1421 (54%)	5674 (55%)	4579 (52%)	637 (30%)
Number (and Percentage) of systems for which security controls have been tested and reviewed in the past year	1330 (51%)	5266 (51%)	4312 (49%)	553 (26%)
Number (and Percentage) of systems for which contingency plans have been tested in accordance with policy	1305 (50%)	5082 (49%)	4234 (48%)	368 (18%)

Table 3: Percentage Frequency by which the Agency logs and monitors activities involving access to, and modification of, critical information

Agency	Percentage Range	
Department of Agriculture	90	100
Department of Commerce	96	100
Department of Defense	91	100
Department of Education	90	100
Department of Energy	91	100
Department of Health and Human Services	71	75
Department of Homeland Security	85	95
Department of Housing and Urban Development	90	100
Department of Justice	100	100
Department of Labor	91	100
Department of State	90	100
Department of the Interior	91	100
Department of the Treasury	90	100
Department of the Treasury	90	100
Department of Transportation	0	10
Department of Veterans Affairs	91	99
Environmental Protection Agency	95	100
General Services Administration	90	100
National Aeronautics and Space Administration	99	100
National Science Foundation	96	100
Nuclear Regulatory Commission	96	100
Office of Personnel Management	91	100
Small Business Administration	100	100
Social Security Administration	90	100
United States Agency for International Development (USAID)	90	100

Table 4: Percentage of Systems Maintaining Audit Trails Providing a Trace of User Actions

Agency	Percentage Range	
Department of Agriculture	90	100
Department of Commerce	85	95
Department of Defense	91	100
Department of Education	90	100
Department of Energy	88	90
Department of Health and Human Services	96	100
Department of Homeland Security	90	95
Department of Housing and Urban Development	90	100
Department of Justice	100	100
Department of Labor	91	100
Department of State	90	100
Department of the Interior	91	100
Department of the Treasury	90	100
Department of the Treasury	90	100
Department of Transportation	10	20
Department of Veterans Affairs	91	99
Environmental Protection Agency	95	100
General Services Administration	90	100
National Aeronautics and Space Administration	99	100
National Science Foundation	96	100
Nuclear Regulatory Commission	96	100
Office of Personnel Management	91	100
Small Business Administration	100	100
Social Security Administration	90	100
United States Agency for International Development (USAID)	100	100

Table 5: Percentage of Systems Operated within the Agency's Incident Handling & Response Capability

Agency	Percentage Range	
Department of Agriculture	99	100
Department of Commerce	96	100
Department of Defense	91	100
Department of Education	90	100
Department of Energy	100	100
Department of Health and Human Services	96	100
Department of Homeland Security	90	95
Department of Housing and Urban Development	90	100
Department of Justice	100	100
Department of Labor	91	100
Department of State	90	100
Department of the Interior	91	100
Department of the Treasury	90	100
Department of the Treasury	90	100
Department of Transportation	85	95
Department of Veterans Affairs	91	100
Environmental Protection Agency	95	100
General Services Administration	100	100
National Aeronautics and Space Administration	99	100
National Science Foundation	96	100
Nuclear Regulatory Commission	96	100
Office of Personnel Management	91	100
Small Business Administration	100	100
Social Security Administration	100	100
United States Agency for International Development (USAID)	100	100

Table 6
For the 25 major agencies, is the New Federal Acquisition Regulation 2008-004 language included in all contracts related to common security settings?

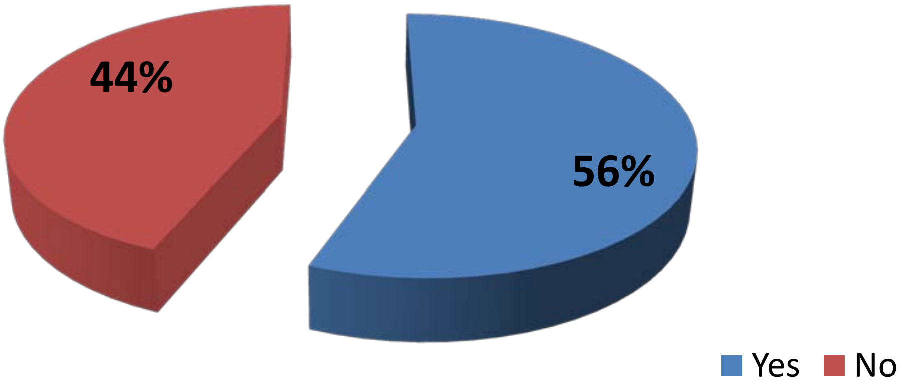


Table 7
Percentage of Agency Workstations & Laptops In Compliance with FDCC

Agency	Percentage Range	
Department of Agriculture	90	100
Department of Commerce	80	90
Department of Defense	91	100
Department of Education	90	100
Department of Energy	71	80
Department of Health and Human Services	96	100
Department of Homeland Security	0	10
Department of Housing and Urban Development	90	100
Department of Justice	80	90
Department of Labor	91	100
Department of State	90	100
Department of the Interior	46	55
Department of the Treasury	90	100
Department of the Treasury	90	100
Department of Transportation	95	98
Department of Veterans Affairs	26	35
Environmental Protection Agency	90	100
General Services Administration	90	100
National Aeronautics and Space Administration	85	90
National Science Foundation	96	100
Nuclear Regulatory Commission	90	100
Office of Personnel Management	0	10
Small Business Administration	90	100
Social Security Administration	90	100
United States Agency for International Development (USAID)	90	100

Table 8: Systems Incident Reporting

Agency	Percentage of the Time the Agency follows documented policies and procedures for identifying and reporting incidents internally?	Percentage of Time the Agency complies with documented policies and procedures for timelines of reporting to US-CERT	Percentage of the time the Agency follow documented policies and procedures for reporting to law enforcement
Department of Agriculture	95% to 100%	95% to 100%	99% to 100%
Department of Commerce	96% to 100%	96% to 100%	96% to 100%
Department of Defense	91% to 100%	91% to 100%	91% to 100%
Department of Education	97% to 97%	95% to 95%	97% to 97%
Department of Energy	100% to 100%	91% to 100%	91% to 100%
Department of Health and Human Services	96% to 100%	96% to 100%	96% to 100%
Department of Homeland Security	90% to 100%	90% to 100%	90% to 100%
Department of Housing and Urban Development	90% to 100%	80% to 90%	90% to 100%
Department of Justice	99% to 100%	99% to 100%	100% to 100%
Department of Labor	91% to 100%	91% to 100%	91% to 100%
Department of State	90% to 100%	90% to 100%	90% to 100%
Department of the Interior	87% to 96%	87% to 96%	87% to 96%
Department of the Treasury	90% to 100%	90% to 100%	90% to 100%
Department of the Treasury	90% to 100%	90% to 100%	90% to 100%
Department of Transportation	90% to 100%	90% to 100%	90% to 100%
Department of Veterans Affairs	91% to 100%	91% to 100%	91% to 100%
Environmental Protection Agency	90% to 100%	90% to 100%	90% to 100%

General Services Administration	96% to 100%	96% to 100%	96% to 100%
National Aeronautics and Space Administration	99% to 100%	99% to 100%	99% to 100%
National Science Foundation	96% to 100%	96% to 100%	96% to 100%
Nuclear Regulatory Commission	96% to 100%	96% to 100%	96% to 100%
Office of Personnel Management	91% to 100%	91% to 100%	91% to 100%
Small Business Administration	100% to 100%	100% to 100%	100% to 100%
Social Security Administration	90% to 100%	30% to 40%	90% to 100%
United States Agency for International Development (USAID)	100% to 100%	100% to 100%	100% to 100%

Appendix 2: National Institute of Standards and Technology (NIST) Performance in 2009

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, Information Technology Laboratory, Computer Security Division (CSD). In 2009, CSD addressed its assignments through the following projects and activities:

- Issued sixteen NIST Special Publications (SP) that addressed management, operational and technical security guidance in areas such as, security controls, system development lifecycle, capital planning and investment, secure content automation protocols, digital signatures, hash algorithms, and cryptographic key management.

- Collaborated 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.

    - Drafted NIST Interagency Report 7621, Small Business Information Security: The Fundamentals, which was released in August 2009. NISTIR 7621 helps small businesses and small organizations implement the fundamental components of an effective information security program.

    - Initiated the development of an outreach video for the Small Business Outreach to help promote IT Security awareness for small to medium sized businesses. This video is now publicly available.

- Reviewed security policies and technologies from the private sector and national security systems for potential federal agency use: Hosted a growing repository of federal agency security practices, public/private security practices, and security configuration checklists for IT products. In conjunction with the Government of Canada's Communications Security Establishment, CSD leads the Cryptographic Module Validation Program

(CMVP). The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate security testing of IT products usable by the federal government.

- Solicited recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines and solicited recommendations of the Board on information security and privacy issues regularly at quarterly meetings.
- Drafted NIST SP 800-126, Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0. [5] The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures that the broadest possible range of use cases is reflected in SCAP functionality.
- 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.

[5] http://csrc/publications/drafts/sp800-126/Draft-SP800-126.pdf