Office of Management and Budget

Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002

TABLE OF CONTENTS

I. Introduction

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). The goals of FISMA include development of a comprehensive framework to protect the government's information, operations, and assets. Providing adequate security for the Federal government's investment in information technology (IT) is a significant undertaking. In fiscal year 2007, the Federal agencies spent $5.9 billion securing the government's total IT investment of approximately $65 billion for the fiscal year 2007 enacted level, equating to approximately 9.2 percent of the total IT portfolio. Funds spent on IT security are used for cross-cutting and system-specific security activities including certification and accreditation (C&A) of systems, testing of controls, and user awareness training.

FISMA assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen IT system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level.

To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with FISMA.

To ensure the safeguard of personally identifiable information (PII), agencies are also required to report on several performance metrics related to information privacy. In addition to tracking the metrics required by the E-Government Act, agencies are also required to report on several additional metrics, including those required by the Privacy Act (5 U.S.C. § 552a), which OMB is charged with implementing.

This report informs Congress and the public of the Federal government's security performance, and fulfills OMB's requirement under FISMA to submit an annual report to the Congress. It provides OMB's assessment of government-wide IT security strengths and weaknesses and a plan of action to improve performance. It also examines agency status against key security and privacy performance measures from fiscal year 2002 through fiscal year 2007.

Data used within this report is based on fiscal year 2007 agency, IG, and privacy reports to OMB. Appendix A contains statistical summaries of security and privacy performance at 25 large agencies. Appendix B provides a summary of small and independent agency compliance with FISMA.

II. OMB Security and Privacy Reporting Guidance

OMB issues reporting guidance to agencies each year to acquire information needed to oversee agency security programs and develop this report.[1] As in the past, this year's guidance included quantitative and qualitative performance measures for the major provisions of FISMA to help identify agency status and progress. Many of this year's security and privacy performance measures are identical to past years' guidance. Based on agency input, some performance measures have been added, modified, or removed since the prior year. Key performance measures remain consistent in order to discern areas of improvement or those requiring improvement from year to year.

OMB's guidance includes specific questions about individual FISMA requirements, including:

- Developing and maintaining an inventory of major information systems (including national security systems) operated by or under the control of the agency, as originally required by the Paperwork Reduction Act of 1995 (44 U.S.C. §101 note). The inventory must be used to support monitoring, testing, and evaluation of information security controls.
- Providing information security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source on behalf of the agency. Agencies using external providers must determine the risk to the agency is at an acceptable level.
- Determining minimally acceptable system configuration requirements and ensuring compliance with them. In addition, agencies must explain the degree to which they implement and enforce security configurations.
- Developing a Plan of Action and Milestones (POA&M) process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. POA&Ms are the authoritative management tool used by the agency (including the IG) to detail specific program and system-level security weaknesses, remediation needs, the resources required to implement the plan, and scheduled completion dates.

Privacy reporting guidance in 2007 requested performance measures to assess agencies' handling of sensitive information, including PII. These performance measures reflect requirements from the E-Government Act, the Privacy Act, and related OMB memoranda. Additionally, agencies were required to provide the URL of the centrally located page on the agency web site listing working links to agency Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). OMB also requested agencies provide copies of each of the four plans developed pursuant to OMB memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

[1] See OMB Memorandum M-07-19 of July 25, 2007, "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf

III. Government-wide Findings

A. Progress in Meeting Key Security Performance Measures

The 25 major agencies of the Federal government continue to improve information security performance relative to C&A rates and testing of contingency plans and security controls. Several larger agencies reported especially notable progress regarding these measures, including the National Aeronautics and Space Administration (NASA), the Departments of State, Treasury, and the Department of Defense (DOD). Agencies have also maintained or improved performance relative to IG qualitative assessments of IT security processes. Federal agencies also showed improvement in IG assessments of the quality of their C&A processes.

Agency FISMA reports also indicate a continued need for improvement in the areas of managing and assigning risk impact levels, employee training in systems security, incident reporting, and oversight of contractor systems.

Table 1 below summarizes overall progress in meeting selected government-wide IT security goals from fiscal years 2002 to 2007.

Table 1: Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2007

Percentage of Systems with a:	**FY 2002**	**FY 2003**	**FY 2004**	**FY 2005**	**FY 2006**	**FY2007**
Certification and Accreditation	47%	62%	77%	85%	88%	**92%**
Tested Contingency Plan	35%	48%	57%	61%	77%	**86%**
Tested Security Controls	60%	64%	76%	72%	88%	**95%**
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	**10,304**

Appendix A provides detail on composite and individual Federal agencies' performance against key security and privacy performance measures as reported in their fiscal year 2007 FISMA submissions to OMB.

Certification and Accreditation

In fiscal year 2007, the percentage of certified and accredited systems rose from 88 percent in 2006 to 92 percent. Eighty percent of the 25 major agencies report a C&A rate between 90 and 100 percent for operational systems. NASA stands out with the most improved C&A performance with an 18 percent increase, while DOD registered another year of continued improvement at 6 percent over the prior year.

Testing of Contingency Plans and Security Controls

FISMA and OMB policy requires agencies to test both system contingency plans and security controls annually. In fiscal year 2007, agencies tested contingency plans for 86 percent of systems and security controls for 95 percent of all systems, up from 77 percent and 88 percent respectively in fiscal year 2006. Five agencies improved contingency plan testing between 20 and 58 percent, including the Department of Education, Department of Homeland Security, the Department of Transportation, the State Department, and the Treasury Department.

Inventory of Systems

Twenty-two of 25 IGs reported their agency's FISMA system inventory was over 80 percent complete, an increase from 20 in 2006. Four agency IGs indicated they do not generally agree with the number of contractor information systems identified in the inventory. The overall inventory decreased by 3 percent from the prior year. Inventory fluctuations were reported by several agencies, including significant inventory decreases at Treasury, NASA, and DHS. Large fluctuations in FISMA inventories, both upwards and downwards, are an indication of immaturity or instability in an agency's process for identifying systems that should be included in the inventory. Also, the inventories of a few agencies dip for the annual reporting cycle, and then rise again in the first quarter FISMA report with a subsequent decrease in C&A rates.

Quality of Certification and Accreditation Process

Seventy-six percent of agency IGs reported the overall quality of C&A processes to be "satisfactory" or better in fiscal year 2007. This is an improvement from 2006, where only 60 percent indicated "satisfactory" or better processes. The number of IGs reporting "poor" processes dropped from 9 to 4 from 2006 to 2007. OMB encourages agency CIOs and IGs to work together to improve the quality of the agency's C&A process, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda (PMA) scorecard, and (beginning in budget year 2009) in assigning projects and investments to the Management Watch List.

Identifying Risk Impact Level

Table 2 below shows the distribution of risk impact levels[2] among agency and contractor systems and their respective C&A rates, contingency plan testing, and security controls testing.

[2] In February 2004, NIST issued Federal Information Processing Standard (FIPS) 199 "Standards for Security Categorization of Federal Information and Information Systems." The standard establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. The process used by agencies to determine FIPS 199 categories is similar to the December 2003 Homeland Security Presidential Directive (HSPD) -7 requirement to identify, prioritize and protect critical infrastructure. Those cyber assets identified as "nationally critical" under HSPD-7 would be categorized as high impact under FIPS 199.

Table 2: Fiscal Year 2007 FISMA System Inventory by Risk Impact Level						
FIPS 199 Risk Impact Level	**Number of Agency Systems**	**Number of Contractor Systems**	**Total Number of Systems**	**Percent certified and accredited**	**Percent with tested contingency plans**	**Percent with tested security controls**
High	1090	121	1211	95%	77%	97%
Moderate	3273	514	3787	92%	90%	96%
Low	4359	334	4693	90%	85%	94%
Not Categorized	229	384	613	94%	91%	98%
Total	**8951**	**1353**	**10304**	**92%**	**86%**	**95%**

Agencies reported a total of 10,304 systems categorized by a risk impact level of high, moderate, low, or not categorized. Of the collective inventory, 8,951 systems were managed by Federal agencies and 1,353 were managed by a contractor or other organization on behalf of a Federal agency. The number of systems categorized as high risk fell by 392 systems (from 1,603 to 1,211 systems), while the number of systems categorized as moderate risk rose by 216 systems (from 3,571 to 3,787).

Systems not categorized by risk impact level remain an issue for agency performance, and represent roughly six percent of the overall FISMA inventory for fiscal year 2007. Though assigning a risk impact level is part of the C&A and risk management process, agencies report a 94 percent C&A rate for uncategorized systems. As these systems are re-accredited, their proper risk impact level should be identified. OMB will focus agency attention on reducing and eliminating uncategorized systems in fiscal years 2008 and 2009.

Employee Training in Systems Security

Agencies reported an overall decrease in the percentage of employees receiving security awareness training, from 91 percent in fiscal year 2006 to 85 percent in fiscal year 2007. Training for employees with significant information security responsibilities increased, however, from 86 percent to 90 percent.

Less than half of the IGs for the 25 large agencies responded “Almost Always (96 to 100 percent of employees)” when asked if the agency has ensured security training and awareness of all employees, including contractors with significant IT security responsibilities. Just over 138,500 employees within the large agencies were reported to have received security awareness training via the Information Systems Security Line of Business (ISSLOB), representing four percent of employees receiving security awareness training in fiscal year 2007.

Incident Reporting

The number of incidents reported by agencies in their annual FISMA reports continues to fluctuate dramatically from the prior year, and continues to vary dramatically from statistics provided by US-CERT. In an effort to clarify and improve FISMA reporting regarding incidents, OMB limited the fiscal year 2007 FISMA annual reporting requirements to the number of incidents reported to USCERT and the number of incidents reported to law enforcement; yet

agencies indicated nearly twice as many incidents reported to USCERT than the Department of Homeland Security reported. Agency IGs indicate most agencies follow procedures for reporting incidents to USCERT and law enforcement, but indicate the identification and subsequent reporting of incidents internally remains an issue at several agencies. These results suggest agency staff may require further training on incident identification and reporting.

Oversight of Contractor Systems

OMB asked IGs to confirm whether the agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy, and NIST guidelines. The number of IGs answering this question as "almost always" decreased from 2006 to 2007 from 15 agencies to 12 agencies.

Agency-wide Plan of Action and Milestones

OMB policy requires agencies to prepare POA&Ms for all programs and systems where a security weakness has been found, and asks agency IGs to evaluate this process. Based on OMB analysis of IG responses in annual FISMA reports, 76 percent of agencies demonstrated they have an effective POA&M process in place for identifying and correcting weaknesses. OMB encourages CIOs and IGs to work together to remediate these process weaknesses, and uses the IGs independent assessment as one factor in assessing an agency's status or progress on the PMA scorecard.

B. Progress in Meeting Key Privacy Performance Measures

As discussed in the sections that follow, the fiscal year 2007 agency FISMA reports indicate limited progress in meeting privacy performance measures.

Table 3: Status and Progress of Key Privacy Performance Measures

	FY 2006	**FY 2007**
Number of systems containing information in identifiable form	2870	3259
Number of systems requiring a PIA	1321	1826
Number of systems with a PIA	1113	1525
Percentage of systems with a PIA	**84%**	**84%**
Number of systems requiring a SORN	1874	2607
Number of systems with a SORN	1555	2169
Percentage of systems with a SORN	**83%**	**83%**

Privacy Program Oversight

In 2007, the majority of agencies report having appropriate oversight of their privacy programs in place. All but one agency reports having a privacy official who participates in privacy compliance activities. Most agencies report privacy training for Federal employees and contractors, with 100 percent reporting general privacy training and 84 percent reporting job-specific privacy training.

Privacy Impact Assessments

The Federal goal is for 90 percent of applicable systems to have publicly posted PIAs. In 2007, 84 percent of applicable systems within the 25 large agencies have publicly posted PIAs. While this percentage remains the same as it was in 2006, the substantial increase in the number of systems identified as requiring a PIA from 2006 to 2007 (an increase of more than 500 systems) is indicative of progress despite no overall increase in the percentage of systems with a PIA.

Quality of Privacy Impact Assessment Process

FISMA reporting guidance for 2007 included a new question for agency IGs concerning the quality of the agency's PIA process. Nineteen of 23 agencies provided an assessment of the PIA process as "satisfactory" or better. Three agencies were reported as having "poor" PIA processes, and one as having a "failing" PIA process. OMB now uses this assessment as one criterion in assigning projects and investments to the Management Watch List.

System of Records Notices

The Federal goal is for 90 percent of applicable systems with PII contained in a system of records covered by the Privacy Act to have developed, published, and maintained SORNs. In 2007, 83 percent of systems government-wide with PII contained in a system of records covered by the Privacy Act have developed, published, and maintained current SORNs. This percentage remains steady from 2006, though the number of systems identified as requiring a SORN increased by more than 700 systems.

Privacy-Related Policies and Plans

Based on the work of the President's Identify Theft Task Force, OMB requested copies of several privacy-related policies and plans in conjunction with agencies' annual FISMA report submission, including:

- Breach notification policy;
- Implementation plan to eliminate unnecessary use of Social Security Numbers (SSN);
- Implementation plan and progress update on review and reduction of holdings of PII; and
- Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

These materials should be made available to the public though means determined by the agency, e.g., posted on the agency web site, by request, etc.

IV. Summary of Government-wide IG Security and Privacy Evaluation Results

Input from the agency IGs is a crucial piece of the annual FISMA evaluation. In addition to assessment and comments in key performance metric areas, OMB annual FISMA reporting guidance asks IGs to assess the quality of the agency POA&M process and C&A process, as well as the completeness of the agency system inventory. The Agency Head has the option to formally over-ride the IGs assessment of these metrics if he or she disagrees with their conclusions. OMB uses these results in designating investments and projects to be included on the Management Watch List, and in assigning agency status and progress scores on the PMA scorecard.

Table 4 below shows a summary of the IG results and assessments for the 25 large Federal agencies for fiscal year 2007. The results of these findings were previously discussed in Section III of this report, Government-wide Findings.

Table 4: Results of IG Assessments for Fiscal Year 2007 FISMA annual report

Agency	Effective POA&M?	Quality of Certification and Accreditation Process	Completeness of System Inventory	Quality of Privacy Impact Assessment Process
Agency for International Development	Yes	Excellent	96-100%	Good
Department of Agriculture	No	Poor	71-80%	Poor
Department of Commerce	Yes	Poor	96-100%	Unaudited
Department of Defense	Unaudited	Unaudited	Unable to determine	Failing
Department of Education	Yes	Satisfactory	96-100%	Satisfactory
Department of Energy	Yes	Satisfactory	96-100%	Satisfactory
Environmental Protection Agency	Yes	Satisfactory	96-100%	Satisfactory
General Services Administration	Yes	Satisfactory	96-100%	Satisfactory
Department of Health and Human Services	Yes	Good	96-100%	Excellent
Department of Homeland Security	Yes	Satisfactory	96-100%	Good
Department of Housing and Urban Development	Yes	Satisfactory	96-100%	Good
Department of the Interior	No	Poor	96-100%	Poor

Table 4: Results of IG Assessments for Fiscal Year 2007 FISMA annual report (continued)

Agency	Effective POA&M?	Quality of Certification	Completeness of System	Quality of Privacy

		and Accreditation Process	Inventory	Impact Assessment Process
Department of Justice	Yes	Excellent	96-100%	Excellent
Department of Labor	Yes	Satisfactory	96-100%	Unaudited
National Aeronautics and Space Administration	No	Good	96-100%	Good
National Science Foundation	Yes	Good	96-100%	Excellent
Nuclear Regulatory Commission	Yes	Failing	81-95%	Excellent
Office of Personnel Management	Yes	Excellent	96-100%	Satisfactory
Small Business Administration	Yes	Satisfactory	96-100%	Satisfactory
Smithsonian Institution	Yes*	Satisfactory	81-95%	Good
Social Security Administration	Yes	Excellent	96-100%	Good
Department of State	No	Satisfactory	96-100 %	Satisfactory
Department of Transportation	Yes	Satisfactory	96-100%	Good
Department of the Treasury	Yes	Satisfactory	51-70%	Satisfactory
Department of Veterans Affairs	No	Poor	81-95%	Poor

*Smithsonian POA&M effectiveness rating determined by Agency Head.

V. OMB Assessment of Agency Incident Handling Programs

A. Incident Reporting

FISMA requires each agency to document and implement procedures for detecting, reporting and responding to security incidents. Agencies must also notify and consult with US-CERT.[3] The Act also requires OMB oversight of the US-CERT and NIST to issue incident detection and handling guidelines.[4]

By including these requirements, FISMA recognizes the Federal government must protect its systems from external threats. While strong security controls can help reduce the number of successful attacks, experience shows some attacks cannot be prevented. Consequently, an effective incident response capability is critical to the government-wide security program as well as individual agency programs.

In May 2005, DHS completed a Concept of Operations for Federal Cyber Security Incident Handling. This document was produced under the auspices of the Cyber Incident Response Policy Coordination Committee, co-chaired by OMB and the Homeland Security Council.

[3] Contact information for US-CERT:
Website Addresses http://www.us-cert.gov https://www.us-cert.gov
Email Addresses soc@us-cert.gov us-cert@dhs.sgov.gov (SIPR) us-cert@dhs.ic.gov (JWICS)

[4] In January 2004, NIST published SP 800-61 "Computer Security Incident Handling Guide."

Agencies' incident handling programs must follow the concept of operations when analyzing and reporting incident data.

The following information is excerpted from the US-CERT annual report for fiscal year 2007:

> In fiscal year 2007, 12,986 incidents were reported to the DHS incident response center for six categories of incidents, which is more than twice the amount of incidents reported the prior year.

Table 5: Incident Reporting to US-CERT

Incident Categories	FY 2005	FY 2006	FY 2007
1. Unauthorized Access	304	706	2,321
2. Denial of Service	31	37	36
3. Malicious Code	1,806	1,465	1,607
4. Improper Usage	370	638	3,305
5. Scans/Probes/Attempted Access	976	1,388	1,661
6. Under Investigation	82	912	4,056
Total Incidents Reported	3,569	5,146	12,986

> Unauthorized access. During fiscal year 2007, incidents involving unauthorized access were responsible for almost 18 percent of total incidents reported. The total number of incidents involving unauthorized access has more than doubled since fiscal year 2006 and seven times more incidents then were reported in 2005 compared to 2007. A further breakdown of this category shows that 85 percent of these incidents resulted from lost or stolen equipment. This is more than a 30 percent increase from the previous fiscal year 2006, with only 50 percent of category one incidents due to stolen equipment. The increase in reporting volume for this type of incident is attributable to mandatory reporting for all cases where PII may have been revealed.
>
> Denial of service. During fiscal year 2007, denial of service incidents decreased by 1 percent. The total number of incidents still made up less than 1 percent of all incidents reported, which is consistent with the previous year's reporting. This category was the only category showing a decrease.
>
> Malicious code. Incidents involving malicious code increased in fiscal year 2007 from the number reported in fiscal year 2006. Although there was about a 10 percent increase from the previous fiscal year, the incident reporting was relatively stable compared to fiscal year 2006 in terms of total volume. Although several new malware threats emerged in fiscal year 07, such as the highly polymorphic and virulent Storm Worm, they have either avoided detection or have not yet impacted the federal agencies at a large enough scale to dramatically increase the total incidents reported.
>
> Improper Usage. During fiscal year 2007, incidents involving improper usage increased more than fivefold. Two-thirds of this total is attributable to the unintentional PII disclosure events from the Department of Veteran Affairs while the remaining one-third consisted of similar cases of PII disclosure reported by other agencies.

Scans/probes/attempted access. During fiscal year 2007, the total number of scans, probes and attempted access incidents increased by 16 percent over the previous year; however, as a percentage of total incidents, it had decreased from the previous year.

Investigation. These incidents are deemed by the reporting entity as unconfirmed and warranting further review as they are potentially malicious or anomalous. This category of incidents showed the largest increase of any category during fiscal year 2007. The total number of incidents filed increased by four fold, and comprised almost 30 percent of all incidents. The reason for this massive increase is intensive analysis of suspicious traffic picked up by the Einstein program sensors.[5] This has enabled US-CERT to identify potential malicious activity and to notify federal agencies of system compromise.

B. Incident Detection

Agencies must be able to quickly detect and respond to incidents. During the next year, OMB will work with federal agencies to increase the exchange of packet level (full content) information regarding incidents which have penetrated an agency's perimeter. Sharing this data will enable more effective analysis of attacks targeting multiple Federal agencies, and may enable more timely responses to new threats. The sharing of intrusion data will also improve the knowledge base of analysts in Federal agencies. In addition, the Einstein program monitors participating agencies' network gateways for traffic patterns that indicate the presence of computer worms or unwanted traffic enabling US-CERT and participating agencies the ability to view nefarious activities going on within the Federal government.

C. Incident Prevention

The threat to US Government systems is shifting from opportunistic hacking to targeted, dynamically adapting attacks. To counter this threat, agencies need to make the best use of existing IT security policies and practices. In addition, a long term architectural roadmap is necessary to provide a consistent strategy for mitigating malicious cyber activity.

NIST has produced comprehensive security guidance for agencies through the SP-800 series of publications. SP800-53 in particular includes very specific instruction around necessary security controls. Agencies should apply the NIST guidance using a baseline architectural roadmap that addresses not only the selection of security controls but the deployment and integration of those controls as part of a comprehensive framework of management, operational, and technical controls.

VI. OMB Assessment of Privacy Management

[5] The Einstein program provides a mechanism for the collection of summary network traffic information at agency gateways and provides a high level view across the federal government network infrastructure.

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

- Develop and implement a breach notification plan, setting forth specific six factors agencies should consider when determining whether and how to respond to breach of data in their possession;

- Implement a plan to eliminate unnecessary collection and uses of SSNs in agency programs and systems;

- Implement a plan and submit a progress update on the review and reduction of unnecessary PII in their possession; and

- Develop specific rules of behavior regarding PII security and the consequences for rule infractions to ensure agency staff knows their responsibilities to safeguard PII.

Based on information provided to OMB as part of the fiscal year 2007 FISMA report, submitted by most agencies on October 1, 2007, agencies have taken significant steps in developing and implementing their breach notification, SSN reduction, and PII reduction plans. In contrast, agencies' development of privacy-specific rules of behavior and consequences often missed the mark as many agencies have only a broad policy to address employee and supervisor misconduct for failures to safeguard sensitive information, are still developing rules of behavior, or have general security-focused rules, but no privacy-specific rules of behavior.

Most agencies have reviewed their SSN holdings and collections and have eliminated unnecessary SSN or are in the process of doing so. A few agencies, however, have only a general policy to reduce SSN or are developing a SSN reduction plan.

Agencies were also asked to report on participation in government-wide efforts to explore alternative identifiers. Some agencies stated they participate in government-wide efforts, but do not specify which ones. Also, several agencies already use, are in the process of developing, or are considering adopting an alternative identifier. More precision on this issue would be helpful.

In some instances, agencies failed to respond fully to the Directive to develop a PII reduction plan and to submit a progress update on minimizing unnecessary PII collections and holdings. For some agencies, the primary sensitive data held or collected is SSNs. For this reason, several agencies' PII reduction plans overlap their SSN reduction plans.

Few agencies responded fully to the Directive to develop privacy-specific rules of behavior and consequences. As of October 2007, several agencies were in the process of developing such rules, while others had developed specific privacy rules, but did not attach any specific consequences to them. Still other agencies had a general policy instructing employees to protect PII, but set forth no specific behaviors or consequences for not doing so. In addition, several agencies submitted security-focused rules of behavior, but failed to address adequately the

privacy concerns. Finally, many agencies did not address behaviors and consequences of supervisors to protect PII in their rules of behavior plans.

VII. Plan of Action to Improve Performance

A. President's Management Agenda (PMA) Scorecard

While IT security clearly has a technical component, it is at its core an essential management function. OMB has increased executive level accountability for security and privacy by including these elements in the PMA scorecard.

The PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government). The goals of the E-Government initiative are to ensure the Federal government's annual investment in IT significantly improves the government's ability to serve citizens, and to ensure systems are secure, delivered on time, and on budget.

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either "green" (agency meets all the standards for success), "yellow" (agency has achieved intermediate levels of performance in all the criteria), or "red" (agencies have any one of a number of serious flaws). IT security is one critical component agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status, regardless of their performance on other E-Government criteria. Similarly, agencies must successfully meet information privacy components to maintain a green rating. Agencies are publicly held accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html.

To "get to green" under the E-Government scorecard, agencies must meet the following three security criteria:

- IG or Agency Head verifies the effectiveness of the Department-wide IT security remediation process;
- IG or Agency Head rates the agency C&A process as "Satisfactory" or better; and
- The agency has 90 percent of all IT systems properly secured (certified and accredited).

In order to "maintain green," by July 1, 2008, agencies must meet the following security and privacy criteria:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations;

- Has demonstrated for 90 percent of applicable systems a PIA has been conducted and is publicly posted;

- Has demonstrated for 90 percent of systems with PII contained in a system of records covered by the Privacy Act to have developed, published, and maintained a current SORN; and

- Has an agreed-upon plan to meet communication requirements for COOP and COG.

OMB will continue to use the E-Government scorecard to motivate agency managers and highlight areas for improvement.

B. Review of Agency Business Cases and Management Watch List

OMB has integrated IT security and privacy into the capital planning and investment control process to promote greater attention to security and privacy as fundamental management priorities. To guide agency resource decisions and assist OMB oversight, OMB Circular A-11, "Preparation, Submission and Execution of the Budget," requires agencies to:

- Report security costs for all IT investments;

- Document adequate security controls and costs have been incorporated into the life cycle planning of each investment; and

- Tie POA&Ms for a system directly to the funding request for the system.

Part 7 (Exhibit 300) of OMB Circular A-11 requires agencies to submit a Capital Asset Plan and Business Case justification for major IT investments. In their justification, agencies must answer a series of security and privacy questions and describe how the investment meets the requirements of the FISMA, E-Government Act, Privacy Act, OMB policy, and NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate. Any business case that fails to receive a satisfactory review of its security information is placed on the Management Watch List.

Beginning with the budget year 2009 submissions of agency Exhibit 300s, OMB formally incorporated three FISMA performance measures into the criteria for projects and investments to be included on the Management Watch List:

- IG assessment of the quality of the agency's C&A process;

- IG review results of the effectiveness of the POA&M process (as defined on page 2 of this report); and

- IG assessment of the quality of the PIA process.

Any agency failing to achieve a "satisfactory" or better assessment of their C&A or PIA process, or failing to achieve an "effective" rating of their POA&M process has all IT investments within the agency portfolio placed on the Management Watch List until they remediate those performance weaknesses.

C. The Information Systems Security Line of Business Initiative

The Information Systems Security Line of Business (ISSLOB) is an interagency effort led by the Department of Homeland Security to identify common security processes and technologies to improve our information security program's performance, reduce costs, and increase efficiency.

The initiative selected three agencies as shared service centers for security awareness training, the Department of Defense, the Office of Personnel Management, and the Department of State – in coordination with the United States Agency for International Development. Additionally, two agencies were selected as shared service centers for security reporting, the Department of Justice and the Environmental Protection Agency.

In November 2007, 12 agencies had implemented security awareness training services provided by the initiative, and 13 agencies had begun using FISMA reporting services provided by the initiative. As a result, agencies reduce duplicative investment in common security tools, ensure a baseline level of training and reporting performance, and can refocus their efforts to other complex and critical security issues at their agency. OMB expects agencies will fully report the number of employees trained via the ISSLOB in their fiscal year 2008 annual FISMA report.

The initiative identified additional security services and tools demanded by agencies, including vulnerability assessment, network mapping and discovery, and baseline configuration management tools. 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 security threats. The initiative is now establishing mechanisms to help agencies quickly acquire these tools in a cost-effective manner.

D. Federal Desktop Core Configuration

OMB issued policy requiring agencies with Microsoft XP and VISTA operating systems, or plans to upgrade to these operating systems, to adopt the Federal Desktop Core Configuration (FDCC).[6] The FDCC was developed in partnership with the National Institute of Standards and

[6] See OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* and OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, at: http://www.whitehouse.gov/omb/memoranda/

Technology, the Department of Homeland Security, the Department of Defense, and Microsoft (for more information see: http://fdcc.nist.gov/).

Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information.

Agencies are now:

- Testing these configurations in a non-production environment to identify adverse effects on system functionality;
- Implementing and automating enforcement when using these configurations;
- Restricting administration of these configurations to only authorized professionals; and
- Ensuring new acquisitions include these configurations and require information technology providers to certify their products operate effectively using these configurations.

E. Top 10 Risks Impeding the Adequate Protection of Government Information

To make the Federal government's identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the President's Identity Theft Task Force issued "Combating Identity Theft: A Strategic Plan." The strategic plan instructed the OMB and the DHS to develop a paper identifying common risks (or "mistakes") and best practices to help improve agency security and privacy programs. The risks, best practices, and important resources are inter-related and complementary. Agencies apply them when administering their information security and privacy programs. The report can be found at: http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf).

F. Privacy Management

The next step in advancing the federal government's response to the President's Identity Theft Task Force recommendations, and OMB implementing directives, is for agencies with draft plans or statements of general policy to finalize their plans. The plans should be made available to the public through means determined by the agency, e.g. posted on the agency web site, by request, etc. To assist agencies in preparing final plans, OMB offers the following suggestions in each of the four privacy areas.

Breach Notification

If they have not done so already, agencies must now finalize any breach notification plans still in development. Further, to ensure quick action in the event of a breach, agencies should develop and have readily available relevant model documents, such as sample breach notification letters to affected individuals, agency news releases, and FAQs.[7] In addition, many, but not all, agencies have committed to accommodate the needs of hearing or visually impaired individuals when issuing breach notices. The remaining agencies may wish to do so when preparing their final breach notification plans.

SSN Reduction

If they have not done so already, all agencies should set forth a specific timetable with milestones for achieving their SSN reduction goals. Agencies should specify the particular alternative identifier approach adopted or under consideration and whether the alternative identifier is used specifically for federal programs, federal employees, or both.

PII Reduction

All agencies must submit a PII reduction progress update with specific milestones and actual completion dates or expected completion dates. Accordingly, agencies lacking complete PII reduction plans or progress updates should prepare them now.

Rules of Behavior

Agencies must review again their rules of behavior to ensure they adequately address three concerns. First, agencies must have complete privacy-specific rules of behavior in place. This means agencies with draft plans or general conduct policies must now develop complete privacy-focused rules of behavior. Broad employee codes or security-focused rules alone will not suffice.[8] Second, if they have not done so, agencies must address rules of behavior for supervisors in particular,[9] which also set forth specific consequences for failing to protect PII. Third, agencies must consider the consequences, or possible consequences, flowing from each specific type of privacy rule infraction.[10]

VIII. Conclusion

Over the past year, agencies continued to make incremental progress in closing the Federal government's IT security performance gaps in the areas of C&A and testing of contingency plans and security controls.

---

[7] For examples of model notification letters, news releases, and FAQs, see the plans submitted by USDA, Education, DHA, Interior, Justice, Labor, and VA.

[8] Examples of rules of conduct can be found in the plan submitted by USDA and the draft plans submitted by Education, Labor, and NASA.

[9] *See* SSA Rules of Conduct (supervisor conduct).

[10] *See* NASA Rules of Conduct (consequences).

Through existing processes, OMB will continue to work with agencies to focus management attention on:

- Achieving 100 percent C&A levels for all operational systems
- Properly identifying and providing oversight of contractor systems;
- Reducing or eliminating systems in the FISMA inventory uncategorized by risk impact levels;
- Improving agency identification and reporting of security incidents;
- Increasing general and job-specific training for Federal employees and contractors;
- PIA and SORN maintenance for 90 percent of applicable systems; and
- Completing recommendations of the President's Identity Theft Task Force.

OMB will continue to work with agencies, IGs, CIOs, GAO, and the Congress to strengthen the Federal government's IT security and privacy programs.

A copy of this report is available at www.whitehouse.gov/omb.