FISMA Report

Fiscal Year 2006

Revision: 3.0

Date: September 29, 2006

Prepared for the Office of Management and Budget

By the Office of the Chief Information Officer

Table of Contents

List of Tables

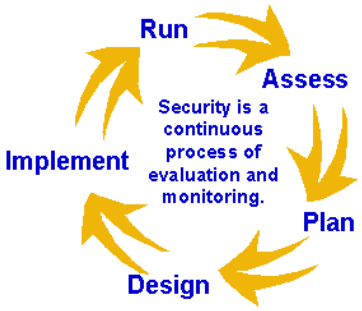
List of Figures

1 Introduction

The Federal Information Security Management Act (FISMA) of 2002 requires the Chief Information Officer of each Federal department to assess and report on the status of his or her information security program. This report meets that requirement and has been prepared according to the Office of Management and Budget (OMB) Fiscal Year (FY) 2006 FISMA reporting instructions.

1.1 Security Continuum

As illustrated below, the United States Department of Agriculture's (USDA's) security posture is in a continuous process of being evaluated, monitored, and improved. The success of USDA's security program depends on vigilance and continuing assessment of the environment coupled with improvements to security policies, procedures, tools, and configuration standards to protect the Department's information and information assets.



The security improvement projects and initiatives outlined in this document have significantly increased the comprehensiveness of, and focus on, information security to management. Accomplishments in FY 2006 included increased management focus and involvement through a variety of programs, including a security program scorecard; enhanced accuracy for information systems and information technology (IT) inventories; improved certification and accreditation (C&A), plan of action and milestones (POA&M) and training processes; automated information systems risk categorization; and improved system and program reviews.

1.2 Objective

One of the primary objectives of the FISMA program is to ensure the effectiveness of information security controls in Federal agencies. Under strong senior leadership, USDA has enhanced overall information security and has addressed material weaknesses identified in FY 2005. The Department also has improved the security of USDA's IT hardware and software assets as well as many areas of USDA's information security program. This document highlights the work performed as part of each improvement initiative and includes input from annual system and program reviews, agencies' work in correcting weaknesses identified in their POA&Ms, and other work performed throughout the FY 2006 reporting period.

2 FY 2006 Highlights

Many improvements have been made in FY 2006. These improvements include:

- Developing a scorecard to focus managers' attention on security and to increase management commitment and monitoring of information security systems
- Implementing the Automated Security Self-Evaluation and Remediation Tracking (ASSERT©) tool to support automated scoring efforts to secure information systems
- Initiating concurrency reviews of new C&A packages
- Performing agency security reviews to identify areas in which improvements are needed
- Implementing a new POA&M tracking process using the ASSERT© tool
- Strengthening the intrusion detection system (IDS) and standard operating procedures
- Improving security awareness training compliance from 62% to over 98%
- Significantly reducing the use of peer-to-peer (P2P) software
- Performing policy gap analyses to determine areas in which further attention to security is needed

These and other efforts have greatly improved the overall USDA security posture in FY 2006. Many components are quantitatively tracked each month on a scorecard to ensure adequate communication with senior management on the progress and status in the areas of security mandated by OMB and FISMA. As a result of this tracking, USDA was able to achieve improved compliance in its quarterly FISMA security reporting by the third quarter of FY 2006.

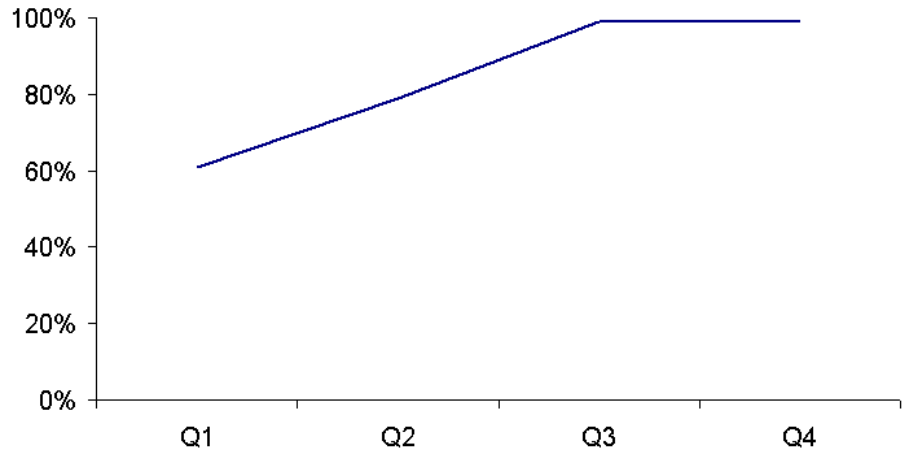


Figure 1. Overall USDA Scores at End of Q1, Q2, Q3, and Q4

Overall views of the scorecard for December 2005, March 2006, and August 2006 are presented below. December 2005 has been included as a baseline for the start of the scorecard initiative. March 2006 has also been selected as a baseline because it marked the first full quarter using the scorecard. August 2006 has been included to provide the most current view of FISMA compliance. Most of the detailed data provided in this report are extracted from agency scorecard data maintained between March and August, 2006. Agencies and OCIO-Cyber Security (CS) work collaboratively to provide updates on scorecard progress. As illustrated by Figures 2, 3, and 4, progressive improvements have been made from each baseline to the present.

		MRP			REE				F&FAS			F,N&CS	FS	NRE		RD	STAFF OFFICES									
		AMS	APHIS	GIPSA	ARS	CSREES	ERS	NASS	FAS	FSA	RMA	FNS	FSIS	FS	NRCS	RD	CR	DA/OO	OBPA	OC	OCE	OCFO	OCIO	OES	OGC	OIG
Overall Agency Grade:																										
Overall Agency Score:		100%	41%	57%	71%	50%	71%	57%	43%	70%	59%	49%	57%	46%	59%	65%	46%	67%	100%	36%	57%	58%	61%	57%	86%	57%
Security Categories																										
1. Certification & Accreditation:	86%	100%	86%	100%	100%	100%	100%	100%	100%	95%	100%	8%	100%	100%	100%	29%	25%	86%	100%	40%	100%	96%	89%	100%	100%	100%
2. POA&M's Resolved (Goal 25%- 1st Quarter)	35%	100%	0%	0%	100%	0%	0%	0%	0%	1%	22%	17%	100%	0%	11%	3%	100%	100%	100%	11%	0%	14%	100%	100%	0%	0%
3. Contingency Planning: (No.# of plans Tested)	52%	100%	0%	0%	100%	50%	100%	100%	0%	95%	88%	0%	0%	19%	100%	21%	0%	86%	100%	0%	0%	96%	37%	0%	100%	100%
4. Monthly Scans 100%	36%	100%	0%	100%	0%	0%	100%	0%	0%	100%	0%	100%	0%	0%	0%	100%	0%	0%	100%	0%	100%	0%	0%	0%	100%	0%
5. Monthly Patches 100% (Critical Patches Applied)	24%	100%	0%	0%	0%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	100%	0%	0%	100%	0%	0%	0%	0%	0%	100%	0%
6. Security Training	^																									
7. Annual Risk Assessments	^^																									
8. Annual Security Plans	^^^																									
9. Verified Systems Inventory	^^^^																									
10. Privacy Act Assessments	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
11. Systems of Records	93%	100%	100%	100%	100%	100%	100%	100%	100%	0%	100%	18%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
12. Configuration Control Board	^^^^																									
TOTAL SCORE:	61%																									

Figure 2. USDA Scores for December 2005

		MRP			REE				F&FAS			F,N&CS	FS	NRE		RD	STAFF OFFICES									
		AMS	APHIS	GIPSA	ARS	CSREES	ERS	NASS	FAS	FSA	RMA	FNS	FSIS	FS	NRCS	RD	CR	DA/OO	OBPA	OC	OCE	OCFO NFC	OCFO FS	OCIO	OES	OGC	OIG
Overall Agency Grade:																										
Overall Agency Score:		92%	67%	61%	75%	77%	94%	88%	64%	72%	82%	50%	84%	68%	82%	84%	56%	81%	100%	78%	73%	89%	90%	80%	87%	94%	77%
Security Categories																										
1. Certification & Accreditation:	89%	100%	89%	100%	100%	100%	100%	100%	100%	95%	100%	15%	100%	100%	100%	100%	60%	86%	100%	40%	67%	93%	100%	89%	100%	100%	100%
2. POA&M's Resolved	76%	100%	75%	0%	100%	20%	100%	80%	0%	100%	100%	0%	97%	26%	100%	100%	100%	100%	100%	100%	0%	100%	100%	100%	100%	100%	73%
3. Contingency Planning: (No.# of plans Tested)	62%	100%	8%	0%	100%	50%	100%	100%	0%	96%	100%	23%	0%	19%	100%	100%	50%	86%	100%	40%	0%	93%	100%	48%	0%	100%	100%
4. Monthly Scans 100%	89%	100%	97%	100%	15%	100%	96%	100%	99%	100%	100%	100%	100%	100%	100%	100%	28%	100%	100%	100%	100%	100%	100%	100%	83%	100%	0%
5. Monthly Patches 100% (Critical Patches Applied)	95%	100%	90%	100%	100%	100%	100%	100%	11%	100%	99%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	83%	100%	97%
6a. CSAT	55%	100%	11%	11%	39%	100%	42%	100%	33%	13%	18%	35%	46%	34%	22%	43%	5%	39%	100%	100%	100%	100%	100%	100%	100%	44%	0%
6b. Specilized IT Training	32%	21%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	100%	0%	0%	0%	0%	0%	100%	0%	100%	0%	0%	0%	100%	100%	100%
7. Annual Risk Assessments	^																										
8. Annual Security Plans	^^																										
9. Verified Systems Inventory (EAR)	^^^																										
10. Privacy Act Assessments	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
11. Systems of Records	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	89%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
12. Configuration Control Board (Charters)	89%	100%	100%	100%	100%	100%	100%	100%	100%	14%	100%	38%	100%	100%	100%	100%	25%	100%	100%	100%	67%	100%	100%	67%	100%	100%	100%

Figure 3. USDA Scores for March 2006

		MRP			REE				F&FAS			F,N&CS	FS	NRE		RD				STAFF OFFICES								
		AMS	APHIS	GIPSA	ARS	CSREES	ERS	NASS	FAS	FSA	RMA	FNS	FSIS	FS	NRCS	RD	ASCR	DA/OO	NAD	OBPA	OC	OCE	OCFO NFC	OCFO FS	OCIO	OES	OGC	OIG
Overall Agency Grade:																												
Overall Agency Score:		91%	85%	99%	100%	92%	99%	100%	99%	99%	92%	99%	99%	99%	99%	99%	92%	92%	91%	92%	100%	100%	99%	100%	99%	100%	100%	99%
Security Categories																												
1. Certification & Accreditation:	100%	100%	95%	100%	100%	100%	100%	100%	100%	95%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
2. POA&M's Resolved	99%	100%	80%	100%	100%	100%	100%	100%	100%	96%	100%	100%	97%	97%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
3. Contingency Planning: (Number of Plans Tested)	97%	100%	23%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
4. Monthly Scans 100%	100%	99%	100%	100%	100%	97%	100%	99%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
5. Monthly Patches 100% (Critical Patches Applied)	99%	100%	96%	100%	100%	100%	100%	100%	99%	99%	99%	100%	100%	100%	99%	99%	100%	100%	100%	100%	100%	100%	100%	100%	100%	96%	100%	97%
6a. CSAT	94%	92%	84%	90%	100%	100%	99%	100%	100%	98%	100%	96%	100%	98%	100%	100%	100%	100%	92%	100%	100%	100%	100%	98%	100%	100%	100%	100%
6b. Specialized IT Training	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
7. Annual Risk Assessments	69%	0%	30%	100%	100%	0%	100%	100%	50%	100%	0%	91%	92%	100%	100%	100%	0%	0%	0%	0%	100%	100%	100%	100%	100%	100%	100%	100%
8. Annual Security Plans	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
9. Verified Systems Inventory (EAR)	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
10. Privacy Act Assessments	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
11. Systems of Records	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%
12. Configuration Control Board (Charters)	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	N/A	100%	100%

Figure 4. USDA Scores for August 2006

Note. See Appendix B, page 30, for a list of acronyms.

3 Fiscal Year 2006 Initiatives

Security improvements in FY 2006 are covered in this section; security initiatives developed to improve overall USDA cyber security posture are documented under Section 4; and security initiatives planned for FY 2007 are covered under Section 5.

3.1 Oversight

3.1.1 Scorecard Program

The Office of the Chief Information Officer (OCIO) scorecard is used to assess the effectiveness of each individual agency's information system security program and to keep USDA senior management informed of progress and status on implementing and maintaining security over IT assets.

Introduced in December 2005 without supporting processes for ongoing data gathering, agreements on metrics, or consensus on presentation, the scorecard has evolved to become the centerpiece in monthly briefings to USDA's management. The scorecard is used for

- Developing and tracking security metrics (e.g., number of systems accredited, percentage of security awareness training completed, contingency plans tested, etc.);
- Exercising oversight through OCIO review of selected performance metrics.

The scorecard program incorporates the President's Management Agenda and provides metrics for agency compliance on information systems inventory, accreditation, patching, training, etc. CS liaisons work with agencies to obtain information and resolve discrepancies between reported information and information obtained from ASSERT©, AgLearn, the enterprise architecture repository (EAR), and scan/patch certifications. The Departmental leadership team (the Deputy Secretary and the Under Secretaries) and agency administrators are then briefed monthly on the scorecard results. In addition, the scorecard results are reviewed monthly by the IT Leadership Council composed of agency CIOs. The scorecard elements are now included in the performance evaluation criteria for each agency's CIO and are used to calculate overall USDA scores to highlight areas of compliance and noncompliance. The OIG review and the Office of the Chief Financial Officer (OCFO) internal control assessment identified areas where OCIO needs to refine the scorecard metrics and to validate the information reported. These areas will be addressed in FY 2007.

3.1.2 ASSERT© Usage

To ensure compliance with National Institute of Standards and Technology (NIST) established standards for assigning risk levels to Federal information systems, OCIO has implemented the ASSERT© tool to provide automatic assignment of required Federal Information Processing Standard (FIPS) 199 security categories (i.e., High, Moderate, or Low Impact) to the systems in the enterprise architecture repository (EAR). Proper security categorization ensures the congruence of security categories with other systems information and provides better management oversight of compliance.

3.1.3 Concurrency Review

In FY 2005, the Office of Inspector General (OIG) identified issues associated with inadequate oversight in the Department's C&A process. To address this issue and strengthen the C&A process, OCIO-CS began independently reviewing certification packages in FY 2006. Systems cannot be accredited until CS reviews the C&A package and provides recommendations to the certifying official. Approximately two dozen concurrency reviews were completed in FY 2006, and OCIO continues to refine the process with each concurrency review. The concurrency review process is still maturing, and procedures and tools are being formalized. The OIG review also identified areas where the concurrency review process and the supporting documentation can be improved. The process is expected to become more rigorous in FY 2007.

3.1.4 Oversight of Information Security Programs

The structure of the USDA OCIO/Cyber Security (CS) is supporting a strong oversight organization, which is codified in Department Manual (DM) 3545-001, "Computer Security Awareness and Training." OCIO has formalized a process for initiating, reviewing, and updating the Department's CS policies to improve its compliance with legislation and regulations. OCIO also has mapped USDA's policies against discrete requirements contained in laws, Presidential directives and regulations; has performed a gap analysis to prioritize any required policy work; and has developed a program to review and update existing departmental cyber security policies based upon changes in legislation and regulations. In addition, OCIO has implemented a security review program to evaluate the accuracy of information provided by agencies and the effectiveness of their security implementations and to provide effective oversight of agency security review programs. OCIO is also in the process of reviewing controls over systems configuration management by evaluating agency configuration control board (CCB) charters.

3.1.5 Agency Security Reviews

FISMA requires all Federal agencies to implement and maintain information security policies, procedures, and control techniques to ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. OIG cited the USDA's Cyber Security Program as a material weakness in FY 2005.

As part of Cyber Security's strategy to resolve this issue and identify areas in which improvement is needed, the CS team is reviewing the security program implementation of all USDA agencies, including major applications and general support systems, in a 2- to 3-year cycle. The purpose of the security review is to determine the completeness, adequacy, and effectiveness of each agency's Cyber Security Program as defined by NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems." The security reviews cover the following assessment areas:

- Access control, awareness and training, audit, and accountability;
- Certification, accreditation, and security classification;

- Management assessments, configuration management, and contingency planning;
- Identification and authentication, incident response, and maintenance;
- Media protection, and physical and environmental protection and planning;
- Personnel security;
- Risk assessment, and system and services acquisition;
- System and communications protection; and
- System and information integrity.

The reviews include activities such as interviews with personnel, review of documents, analysis of logical security controls, and observation of practices and physical controls. CS has completed eight agency security reviews so far in FY 2006. Two additional reviews are in progress and should be completed by the end of September, 2006. These two reviews are focusing on the verification and validation of agency POA&M closure and POA&M close-out procedures.

3.1.6 Configuration Control Board (CCB) Charters

As part of its oversight function, CS verifies that a CCB is chartered to provide managers, users, technicians, and other stakeholders with a formal voice in the evolution, plans, and schedules associated with the development, operation, maintenance, and retirement of information systems supporting the organization's business goals for all systems reported. The actual process is reviewed during agency security reviews and interviews. CS will be performing additional verification in FY 2007 by reviewing charters as well as the CCB process. The number of systems covered by CCB charters for each agency as of August 31, 2006, is tracked in the monthly scorecard and presented below.

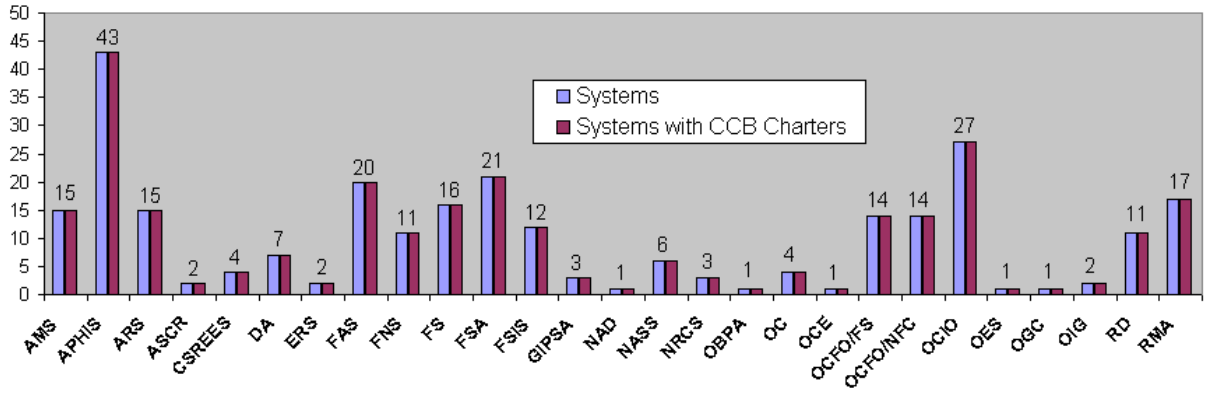


Figure 5. Systems Covered by CCB Charters as of August 31, 2006

3.2 Certification and Accreditation

3.2.1 C&A

Certification, made in support of security accreditation, involves a comprehensive assessment of management, operational, and technical security controls in an information system and determines the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system.

Accreditation refers to the official management decision given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, and reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.[1]

The successful completion of C&A provides agency officials with the necessary assurances that the information system has appropriate security controls and that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing. In essence, C&A provides a form of quality control that challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints, and mission requirements. C&A documentation is reviewed during the concurrency review process; however, the OIG review identified areas where improvement in OCIO oversight can be made in FY 2007.

The following chart compares the total number of systems and systems accredited for each agency as of August 31, 2006.

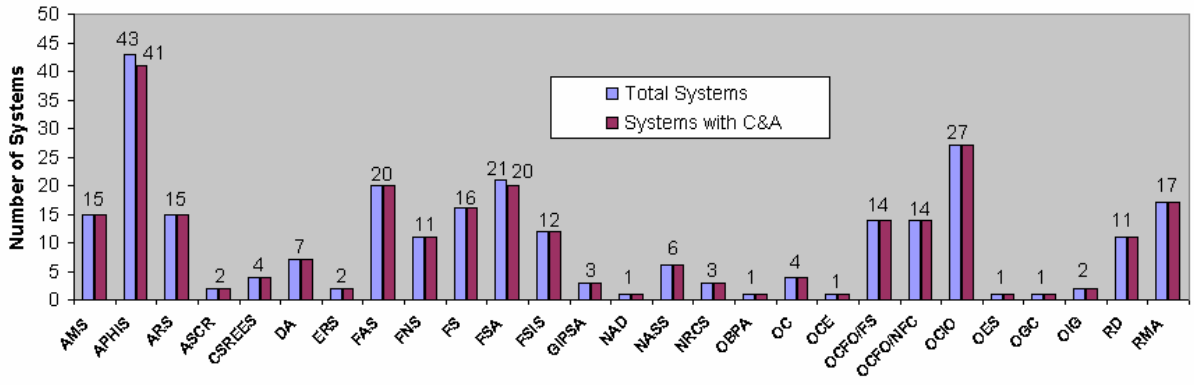


Figure 6. Agency Systems with C&A as of August 31, 2006

[1] NIST Interagency Report 7298, Glossary of Key Information Security Terms.

3.2.2 Plan of Action and Milestones

Federal regulations and guidelines require plans of action and milestones to be developed to mitigate security risks. In response to the OIG recommendations to improve management and reporting of POA&Ms, USDA replaced its POA&M database with the ASSERT© tool to provide more robust reporting and management capabilities. As of the first quarter's FISMA report, less than 15 percent of the POA&Ms had been completed. As of August 31, 2006, over 98 percent had been completed. ASSERT© also generates FISMA performance measurements at the system level and collects and maintains data for quarterly and annual FISMA reporting to OMB. CS is planning to expand the use of the ASSERT© tool to provide independent review and closure of POA&Ms. CS is also integrating Security Reviews with the POA&M process. Two security reviews have focused on the POA&M closure process to assure that POA&Ms are closed appropriately. One of OCIO's areas of emphasis for FY 2007 will be to ensure that all POA&Ms are reported in the ASSERT© tool – an issue identified by OIG and OCFO reviews.

3.2.3 Systems Consolidation

USDA is working to consolidate and reduce its systems inventory. Consolidation will not change accreditation boundaries in a physical sense but will provide a more manageable virtual view. This USDA effort is meant to balance the need for practical, cost-effective system and security boundaries with the requirements of disparate functions that would make the security C&A process extremely unwieldy, expensive, and complex. NIST guidance gives agencies great flexibility in determining what constitutes an information system (i.e., a major application or general support system) and the resulting security accreditation boundary that is associated with that system.

Using this guidance, USDA reduced the over 400 systems reported in the FISMA FY 2005 report to under 275 in the current report. ARS, in particular, has reduced its systems inventory from nearly 200 to less than 20. FAS has reduced its inventory in the EAR as of August 31, 2006, by approximately half. The primary reduction of systems has been accomplished by decommissioning systems and redefining accreditation boundaries. CS has provided oversight and plans to continue providing oversight in systems consolidation efforts to ensure that the boundaries are appropriate.

3.3 Contingency Planning

FISMA requires plans and procedures to be in place to ensure continuity of operations (COOP) in the event of a loss of service, and OMB requires contingency planning to establish and periodically test a department's capability to continue providing service within a system.[2] In addition, the USDA requires the use of DM 3570-000[3] to guide its IT development of contingency and disaster recovery plans and procedures.

USDA is continuing to make progress for contingency planning. As of August 31, 2006, about 99 percent of agency systems had contingency plans, and about 92 percent of those

[2] OMB A-130, Appendix III, "Security of Federal Automated Information Systems".
[3] DM 3570-000, "IT Contingency and Disaster Planning".

systems had tested plans. In 2005, only about 54 percent of identified USDA systems had completed contingency plan testing.

USDA continues to work toward assuring that all contingency plans are documented in the enterprise Living Disaster Recovery and Planning System (LDRPS). LDRPS is designed for COOP, disaster recovery, and business resumption. USDA's goal is to ultimately test and reference all agency business resumption and disaster recovery plans through the LDRPS enterprise system.

The majority of these plans currently reside in LDRPS. CS is currently in the process of reconciling LDRPS, EAR, and CS C&A databases to ensure that all agencies have the required contingency plans stored in the LDRPS.

3.4 Scanning and Patching

By including metrics for scanning and patch management on the monthly USDA Security Program Scorecard, OCIO has been able to improve monitoring, reporting, and agency compliance with the USDA mandatory monthly network vulnerability scanning and patching certification policy. In FY 2005, only five agencies reported that they had completed the required monthly vulnerability scanning and patching. As of August 31, 2006, however, all USDA agencies have submitted their scanning and patching certifications. The process is still maturing and improving as CS and agencies work together toward compliance. To further facilitate scanning and patching certification, OCIO has created a single certification form to be submitted by the agencies quarterly. The results of the monthly scanning and patching efforts for March through August 2006 are presented in the tables below.

Table 1. Scanning Results (March to August, 2006)

Agency	March 2006	April 2006	May 2006	June 2006	July 2006	August 2006
AMS	100%	100%	100%	100%	100%	100%
APHIS	97%	97%	99%	99%	99%	99%
ARS	15%	16%	100%	100%	100%	100%
CR/ASCR	28%	28%	100%	100%	100%	100%
CSREES	100%	100%	100%	100%	100%	100%
DA	100%	100%	100%	100%	100%	100%
ERS	95%	95%	100%	98%	98%	97%
FAS	99%	99%	99%	99%	99%	99%
FNS	100%	100%	100%	100%	100%	100%
FS	100%	100%	100%	87%	74%	100%
FSA	100%	100%	100%	100%	95%	100%
FSIS	100%	100%	100%	100%	100%	100%
GIPSA	100%	100%	100%	100%	100%	100%
NAD	No Data	100%	100%	100%	100%	100%

Agency	March 2006	April 2006	May 2006	June 2006	July 2006	August 2006
NASS	100%	100%	100%	100%	100%	100%
NRCS	100%	100%	100%	100%	100%	100%
OBPA	100%	100%	100%	100%	100%	100%
OC	100%	100%	100%	100%	100%	100%
OCE	100%	100%	100%	100%	100%	100%
OCFO/FS	100%	100%	100%	100%	100%	100%
OCFO/NFC	100%	100%	100%	100%	100%	100%
OCIO	100%	100%	96%	99%	98%	100%
OES	83%	100%	100%	100%	100%	100%
OGC	100%	100%	100%	100%	100%	100%
OIG	0%	0%	100%	100%	100%	100%
RD	100%	100%	100%	100%	100%	100%
RMA	100%	100%	100%	100%	100%	100%

Table 2. Patching Results (March to August, 2006)

Agency	March 2006	April 2006	May 2006	June 2006	July 2006	August 2006
AMS	100%	100%	100%	100%	100%	100%
APHIS	90%	97%	98%	97%	96%	96%
ARS	100%	100%	100%	100%	100%	100%
CR/ASCR	100%	100%	100%	100%	100%	100%
CSREES	100%	100%	100%	100%	100%	100%
DA	100%	100%	100%	100%	100%	100%
ERS	100%	100%	100%	100%	100%	100%
FAS	11%	59%	96%	97%	88%	99%
FNS	100%	100%	100%	100%	100%	100%
FS	100%	97%	100%	100%	100%	100%
FSA	100%	100%	100%	100%	99%	99%
FSIS	100%	100%	100%	100%	100%	100%
GIPSA	100%	100%	100%	100%	100%	100%
NAD	No Data	100%	100%	100%	100%	100%
NASS	100%	100%	100%	100%	100%	100%
NRCS	100%	100%	100%	100%	100%	99%
OBPA	100%	100%	100%	100%	100%	100%
OC	100%	100%	100%	100%	100%	100%

Agency	March 2006	April 2006	May 2006	June 2006	July 2006	August 2006
OCE	100%	100%	100%	100%	100%	100%
OCFO/FS	100%	100%	100%	100%	100%	100%
OCFO/NFC	100%	100%	100%	100%	100%	100%
OCIO	100%	100%	99%	99%	99%	96%
OES	83%	100%	100%	100%	100%	100%
OGC	100%	100%	100%	100%	100%	100%
OIG	97%	97%	100%	100%	100%	97%
RD	100%	100%	100%	100%	100%	99%
RMA	99%	100%	100%	100%	100%	99%

3.5 Incident Detection

3.5.1 Improving Incident Handling

USDA has been improving its incident handling program, responding to incidents in a timely fashion, and aligning the incident handling process with FISMA requirements. The USDA DM 3505-000, "USDA Computer Incident Response Procedures Manual," is based on NIST SP 800-63, "Recommendation for Electronic Authentication," guidance. To ensure investigation, reporting, and closure of security incidents in a consistent and timely manner, OCIO uses an incident tracking system and identifies the incidents in its weekly activities report, along with incident type, status, and date of occurrence. OCIO is in the final process of formalizing its incident tracking process and establishing controls to ensure that agencies promptly investigate and report on security incidents identified by the Department's intrusion detection system.

3.5.2 Strengthening Standard Operating Procedures

A standard operating procedure (SOP) has been created and updated to assist the USDA Computer Incident Response Team (CIRT) in processing reports of computer security events. The SOP is designed to assist the security analyst in determining which events should be elevated to incidents and which should be referred outside of the USDA CIRT. Procedures for dealing with different types of events and incidents, bringing incidents to the attention of senior officials ("escalation"), and facilitating CIRT interactions with other organizations, both internal and external to the Department, have also been included as part of the SOP. The new SOP includes the following:

- USDA CIRT Incident Management
- USDA CS Reporting Process and Procedure of Computer Security Events
- General Flow of Work/Operating Procedures
- Escalation Procedures
- USDA Incident Contact List

- Form for Reporting Incidents to Cyber Security

3.6 Training

All USDA agency personnel, contractors, and system users must receive information assurance awareness training per USDA DM 3545-001, "Computer Security Awareness and Training," which is in compliance with FISMA mandates. Security awareness compliance was poor in 2005 for several reasons, including technical access issues; lack of eAuthentication credentials; a learning curve in transitioning from GoLearn to AgLearn; and lack of a vehicle for use by management to monitor overall user course completion rates.

In response, OCIO has designated AgLearn, USDA's enterprise-wide online learning management system, as the primary training vehicle with which to increase user security awareness. The USDA Security Literacy and Basics Course was updated in January 2006 and made available via compact disc (CD). OCIO has issued guidance requiring a waiver request signed by the business unit head and approved by the Associate Chief Information Officer (ACIO) of Cyber Security before manual CD security training can be substituted for AgLearn training. The use of the AgLearn system continues to increase the completion rates for mandatory basic security awareness training among USDA employees and contractors. Executive training in FY 2007 will be provided through an IT summit as well as other means. In addition, the CSAT and Privacy training modules will be combined in FY 2007.

OCIO has included performance metrics for security awareness training on the USDA Security Program Scorecard to focus management attention on completion rates. These metrics specifically address computer security awareness training (CSAT) and specialized IT training. Privacy training for all personnel (due September 15, 2006) is also being tracked. Completion rates for the basic security awareness training rose from 54 percent in FY 2005 to over 95 percent currently in FY 2006. The breakdown for CSAT and specialized IT training (percentage) compliance by agency as of August 31, 2006, is shown below.

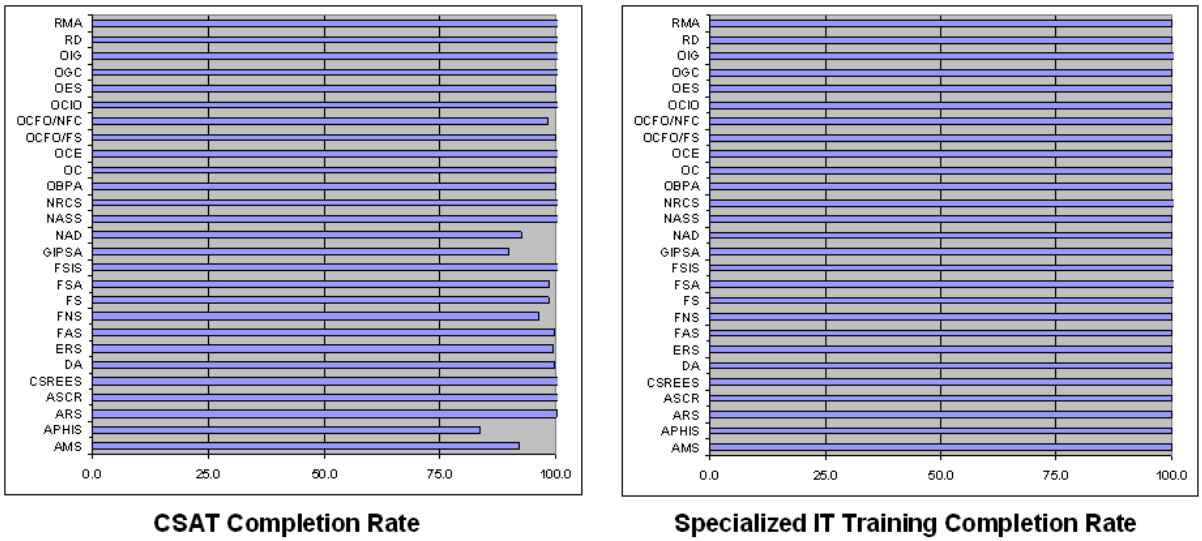


Figure 7. Training Completion Rate as of August 31, 2006

3.7 Peer-to-Peer Tracking

Use of peer-to-peer (P2P) software has been significantly reduced by highlighting its use and explaining its impact to management in the weekly activities report. P2P is a protocol often used to obtain freeware, shareware, and bootleg software. P2P file sharing can potentially compromise computer systems, and the use of this protocol creates vulnerabilities by providing a means of introducing malicious code and other illegal material into a Government network. The use of P2P software is prohibited on all USDA equipment and networks without explicit authorization. USDA Cyber Security monitors all USDA networks for P2P traffic to enforce DM 3525-002, "Internet Use and Copyright Restrictions." A P2P incident table quantifies the number of unauthorized P2P traffic incidents that agencies experience each week. The objective of the report is to bring these incidents to each agency's attention so that a review can be made to determine whether these incidents are potentially detrimental. Since its incorporation into the weekly activities report, agencies have been reviewing P2P incidents and reducing unauthorized P2P traffic and use.

3.8 Self-Assessments

FISMA requires periodic risk assessment to determine the likelihood and magnitude of harm to an agency or organization. USDA DM 3540-002, "Risk Assessment and Security," and DM 3540-001, "Risk Management Methodology," catalog and describe USDA's risk assessment process in detail. Both department manuals require annual reporting from the CIO as part of an annual self-assessment of risk. The self-assessment methodology and checklist facilitates the CIO's reporting of the risk and effectiveness of the agency information assurance (IA) program annually. Agencies are required to perform self-assessments on an annual basis and to report their progress during Q4. The following graph shows the percentage of self-assessments completed for each agency as of August 31, 2006.

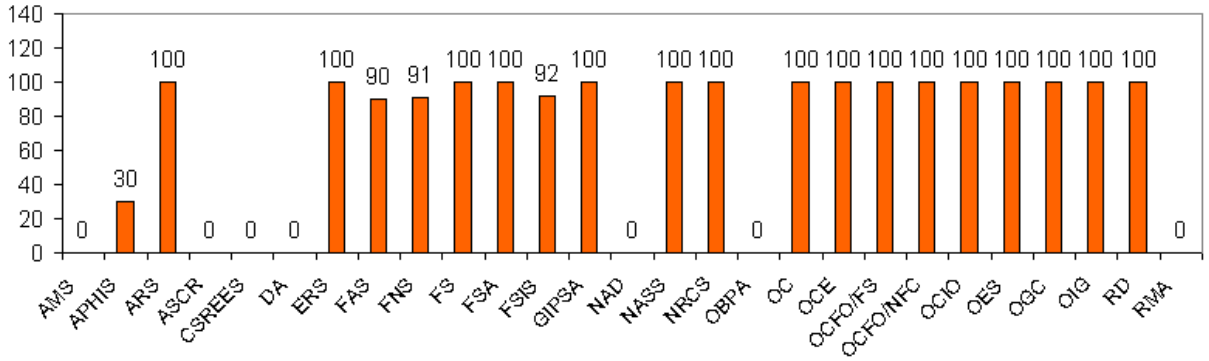


Figure 8. Annual Self-Assessment: Percent Complete as of August 31, 2006

3.9 Annual Security Plans

IT Security Plans are the foundation documents for the overall security process because they define system security features and controls and support capital planning and investment control (CPIC), FISMA reporting, system life cycle efforts, risk management activities, and C&A of IT systems. Therefore, it is critical that they are prepared and updated on an ongoing, annual basis with the most current agency information security practices. Annual security plans are reviewed as part of agency security reviews. The priority for USDA in FY 2006 was to focus on security programs that implement financial systems. Thus, 10 agency security reviews had been conducted for FY 2006 to verify compliance and identify weaknesses in security plans.

To assure compliance with FISMA and OMB A-130, Appendix III, "Security of Federal Automated Information Systems," the number of systems requiring annual security plans and the number of completed annual security plans are tracked on the monthly OCIO scorecard for agencies. As of August 31, 2006, all agencies were in compliance with this requirement.

3.10 Systems Inventory

An accurate inventory ensures that the Department is fully cognizant of all IT assets in order to manage them effectively. The EAR, the official systems inventory of OCIO, was implemented in FY 2006 to address a material weakness identified in FY 2005. The EAR has been developed to manage the inventory of application and general support systems. OCIO cross-references the systems in the EAR to the FISMA inventory of systems to ensure accuracy.

The presence of a verifiable system inventory has been included as a metric on the monthly scorecard. The EAR inventory information is uploaded to the ASSERT© tool to support automated scoring of efforts to secure information systems (e.g., C&A, system categorization, security self-assessment, contingency planning and testing, etc.). The number of systems in the EAR by agency as of August 31, 2006, is presented below.

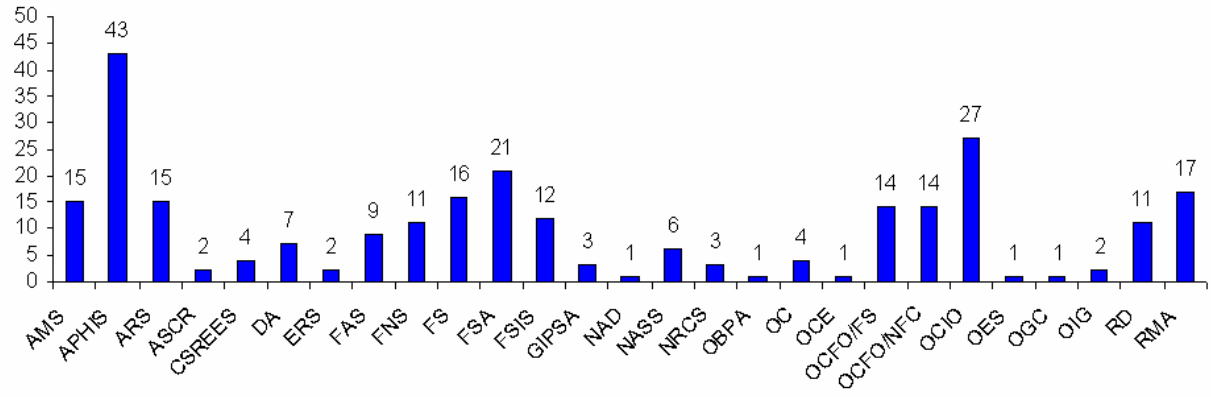


Figure 9. Number of Systems in Enterprise Architecture Repository by Agency

Note: FAS has 9 systems after consolidating the 20 systems shown in Figure 4.

3.11 Privacy

3.11.1 Privacy Act Tracking

The Cyber Security incident response process is used to track and follow up on Privacy Act violations, data compromises, and security breaches as well as lost and stolen computer equipment. OMB requires the reporting of any potential or confirmed Privacy Act compromises to the US-Cert within one hour of its occurrence. The CS tracking and follow-up processes have been established, documented, and tested and are a logical choice for expanding to include Privacy Act data. Thus, a field has been added in the Computer Security Operations database to flag incidents that involve Privacy Act data.

3.11.2 Privacy Act Assessments

Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. Agencies are responsible for initiating the privacy impact assessment (PIA) in the early stages of a system's development to ensure that the PIA is completed as part of the required system life cycle (SLC) reviews. This applies to all of the development methodologies and system life cycles used in USDA. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. To monitor and ensure compliance, the number of systems requiring a Privacy Act assessment and the number of systems completing a Privacy Act assessment is tracked on the OCIO scorecard on a monthly basis. In addition, privacy policy and procedure reviews will be conducted as part of an overall, comprehensive privacy program to ensure that all privacy-related information are captured, tracked, and protected.

3.11.3 Systems of Records

The Privacy Act requires that if information is retrieved by reference to a personal identifier, then the agency must publish current Federal Register notices of the nature and existence of those "systems of records" (SORs). In addition, the Privacy Act has restrictions on disclosure of the records and has fair record keeping procedures regarding access to and amendments to the records. These notices can be found in the Federal Register and on the Government Printing Office website in a compilation that is published every 2 years. The number of SORs and system notices published in the Federal Register for each agency as of August 31, 2006, are shown in the table below.

Table 3. Agency Systems of Records Status as of August 31, 2006

Agency	SORs	SORs Published	Agency	SORs	SORs Published
AMS	1	1	NASS	0	0
APHIS	5	5	NRCS	1	1
ARS	0	0	OBPA	0	0
CR	2	2	OC	0	0
CSREES	1	1	OCE	0	0

Agency	SORs	SORs Published	Agency	SORs	SORs Published
DA	0	0	OCFO/FS	7	6
ERS	0	0	OCFO/NFC	7	0
FAS	15	15	OCIO	2	2
FNS	9	9	OES	0	0
FS	0	0	OGC	0	0
FSA	17	17	OIG	1	1
FSIS	0	0	RD	11	11
GIPSA	0	0	RMA	12	12
NAD	0	0			

3.12 Intrusion Detection System Improvements

USDA's intrusion detection system (IDS) has been strengthened, and upgrades are in progress. In March 2006, CS began to redeploy the sensors within the backbone network. CS plans to upgrade sensor software and hardware in 2007 with appliance servers, which are easier to maintain and manage.

4 Other Improvement Initiatives

In addition to the initiatives discussed in the previous section, OCIO is working on six other major initiatives to improve security for the Department. The six initiatives are depicted below, and details are included in the subsequent subsections.

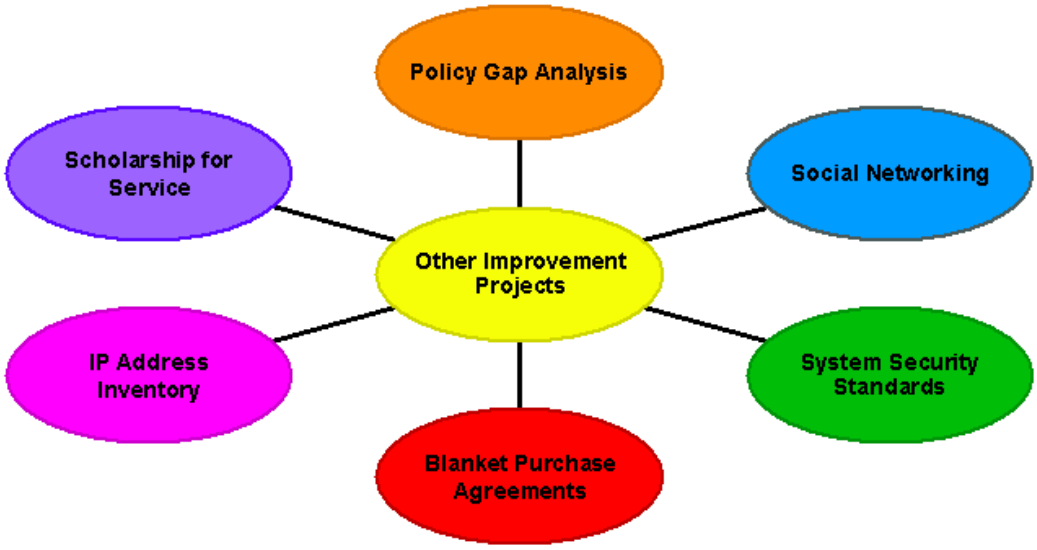


Figure 10. Other Security Improvement Initiatives

4.1 Policy Gap Analysis

A policy gap analysis between FISMA mandates and USDA policy has been performed. The goals and objectives of the FISMA mapping process are to:

- Determine the correlation between USDA policy, guidance and procedures and FISMA mandates;
- Identify other applicable Federal mandates and laws that may pertain to FISMA mandates (e.g., OMB, public law);
- Determine the information assurance category of particular mandates; and
- Make suggestions for perceived weaknesses resulting from the analysis.

Overall, USDA has a strong policy in place that correlates well with FISMA, and its policy is compliant with the following areas of FISMA:

- Program development (reference: DM 3545-002)
- Training (reference: DM 3545-001)
- Oversight (reference: DM 3545-001)
- Senior agency officials' awareness (reference: DM 3545-001 and executive briefing book developed in 2004)
- Annual CIO reports (reference: DM 3540-002 and DM 3540-001)
- Periodic risk assessment (reference: DM 3540-002 and DM 3540-001)
- Risk assessment policies and procedures (reference: DM 3540-002 and DM 3540-001)
- Subordinate plans for networks, facilities, and systems (reference: 3300 series, 3400 series and several other polices for subordinate planning)
- Security awareness training (reference: DM 3545-001)
- Procedures for detecting, reporting, and responding to security incidents (reference: DM 3505-000 and NIST 800-63)
- Plans and procedures to ensure continuity of operations (reference: DM 3570-000)

The policy is partially compliant with requirements for periodic testing and evaluation of information system (IS) policies, procedures, and practices; for planning, implementing, evaluating, and documenting remedial action for deficiencies in IS; and for having sufficient personnel trained to ensure agencywide information assurance coverage. OCIO will address these policy gaps in FY 2007.

4.2 System Security Standards

CS will continue maintaining and adhering to security requirements from NIST and National Security Agency (NSA). System security standards (based on NIST and NSA) include checklists for:

- Classified Systems;

- Telecom Security;
- UNIX Security;
- USDA Mainframe, NT Server, Personal Electronic Devices (PEDs), and Webfarm;
- USDA Windows 2000 Server, Workstation, and Domain Controller Server;
- USDA XP Professional; and
- USDA Novell NOS Security

4.3 Blanket Purchase Agreements

USDA has divided its C&A activities into two primary phases:

- **Phase 1 – Certification.** Phase 1 includes all the activities required to prepare for, rank and assess risk, and plan security for a new or modified information system.
- **Phase 2 – Security Testing & Evaluation.** Phase 2 includes all the steps required to test and document testing of the security controls identified in Phase 1 and to authorize a system for operation.

Prior to having a system accredited, OCIO must perform a mandatory concurrence review to ensure that all identified risks have been mitigated and any residual risks are documented for review by the accrediting official.

To assist agencies with this C&A process, Blanket Purchase Agreements (BPAs) are currently being established with vendors. This contract vehicle will help agencies by providing vendors to perform the necessary phases of certification and accreditation.

4.4 IP Address Inventory

To address a material weakness noted in FY 2005, the OCIO is developing a database that includes accurate, up-to-date contacts for each USDA IP address. The hardware has been delivered, the IP addresses have been loaded into the system, and the required tests have been conducted as part of the pilot. OCIO implemented the IP database in September 2006.

In addition, a field has been added to the database to track IP addresses of systems that contain Privacy Act data. When Computer Security Operations (CSO) receives notification that a system is compromised and the IP address indicates that it contains privacy data, CSO can take precautionary measures such as blocking additional traffic to and from the system, escalating the incident to senior management, etc. [Information withheld under FOIA Exemption 2].

4.5 Scholarship for Service

Scholarship for Service (SFS) is a unique program designed to increase and strengthen the cadre of Federal information assurance professionals who protect the Government's critical information infrastructure. This program provides scholarships that fully cover the typical costs that students incur for books, tuition, and room and board while attending an approved institution of higher learning.

CS is utilizing SFS interns to revitalize the office with recent academic knowledge of information assurance. Candidates are preselected for the program and must have strong academic backgrounds in information security applicable to the Federal sector. As part of the program, the intern will have responsibilities for reviewing and making recommendations on CS policy and for providing information assurance. Selected graduate students must complete 10 weeks of internship and work for the Federal Government for 2 years in return for their scholarships.

5 Planned Improvements

New initiatives to improve security and service for the Department include the programs and processes illustrated below.

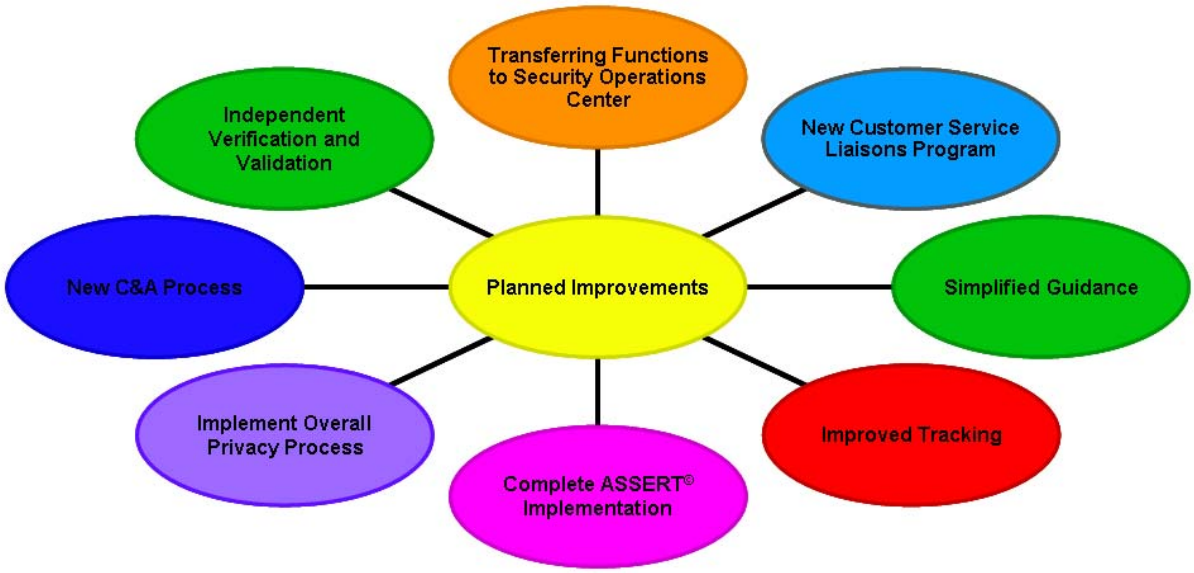


Figure 11. Planned Improvements

5.1 Transferring Functions to Security Operations Center

A security operations center (SOC) that centrally manages and monitors the network and security systems across the diverse USDA IT environment is being developed. The objectives of the SOC are to reduce risk and downtime by implementing tools to actively report security incidents in real time; to control and prevent threats by implementing enterprise-wide intrusion prevention systems (IPS) and IDS; to enable fast and effective incident response and recovery; to establish an effective computer forensics lab for investigating security incidents in order to provide a technical defense against similar future attacks; and to implement a centralized CCB. [Information withheld under FOIA Exemption 2]. The SOC, which will be staffed around the clock, will monitor IDS and other security system functions to be developed.

5.2 New Customer Service Liaison Program

The Cyber Security Liaison Program has changed dramatically in the last year. Increased demands from the OMB and OIG, new guidelines from NIST, and efforts to improve the security program at USDA have all contributed to accelerating changes. To ensure that the Office of the Associate Chief Information Officer (ACIO) for CS serves the agencies' needs for cyber security support while assuring that the Department meets its cyber security goals now and in the future, the Information Security Division (ISD) has developed a new model for liaison support.

The purpose of the new liaison project is to improve communication and collaboration and to build an internal, cohesive, and cooperative team of professionals for a new reorganized CS Customer Service Liaison Program. The program will provide uniform, robust cyber security support. To increase the likelihood of success, CS has developed a customer survey to obtain information from USDA agencies regarding current support and service and to solicit ideas for improvements. To assure that high-quality customer service is provided, CS will continuously monitor the questions received and the answers provided. This will help assure that consistent answers are given, appropriate tools are developed to assist the agencies, and high-quality customer support is provided.

The new Customer Service Liaison Program will provide a centralized, standardized, and formal structure for handling inquiries and for tracking and monitoring progress toward resolving customer issues. In addition, the program will:

- Provide efficient, timely, and improved services to customers.
- Improve collaboration, communication, and cooperation as the CS team works together to provide consistency, knowledge, experience, and an environment receptive to feedback for improving cyber security USDA-wide.
- Establish a central telephone number with voice mail to handle phone inquiries.
- Establish a web page as an alternate way to submit inquiries.
- Establish routine quarterly visits with customers with a planned agenda, and provide trip reports of findings and recommendations.

The new Customer Service Liaison Program will also include full-time liaison representatives to service customers 5 days a week.

5.3 Independent Verification and Validation Plans

The FY 2007 scorecard will require that agencies complete FISMA deliverables by the end of the third quarter of the fiscal year. This will provide OCIO with time for the completion of all FISMA-related deliverables by the end of the fiscal year as well as sufficient time for extensive independent verification and validation by CS of these deliverables.

5.4 Simplified Guidance

Agencies will be submitting information on their systems using simplified, combined guidance for C&A and concurrency reviews in FY 2007.

5.5 Improved Tracking

CS will include new elements in the monthly scorecard to better track financial systems and any A-123 issues for those systems. CS is working to prepopulate special factors, if applicable, to ensure that such factors are appropriately included for all like systems.

5.6 Complete ASSERT© Implementation

CS will be working to complete the ASSERT© implementation in FY 2007 as follows:

- Finalize and publish procedures to ensure the ASSERT© systems inventory is synchronized with the EAR;
- Obtain Agency CIO approval for final system categorization and security self-assessments in ASSERT©;
- Convert self-assessments based on ASSERT© NIST SP 800-26, “Security Self-Assessment Guide for Information Technology Systems,” to NIST SP 800-53, “Recommended Security Controls for Federal Information Systems,” controls;
- Implement continuous monitoring of NIST 800-53 security controls in ASSERT©; and
- Integrate ASSERT© and Management Initiatives Tracking System (MITS) security-related data collection and reporting.

5.7 Implement an Overall USDA Privacy Process

An overall USDA Privacy process will be implemented in FY 2007 as follows:

- Draft an overall privacy process with major stakeholders (newly designated Agency Privacy Officers, Agency CIOs, Information Systems Security Program Managers (ISSPMs), Office of the Executive Secretariat (OES) personnel, the IT Project Manager, etc.);
- Identify data points and sources and establish a data repository for all required privacy reporting and reviews;
- Develop and publish a 3-year calendar of required privacy reviews and reports to OMB; and
- Implement monthly meetings with newly designated Privacy Officers.

5.8 New C&A Process

The revised C&A process will:

- Use NIST 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," as the basis and structure for the new USDA C&A policy, procedure and guidance;
- Add additional requirements, documents, and ACIO-CS oversight to ensure proper C&A for the diverse USDA agencies;
- Focus on utilizing the expertise found in ACIO-CS for independent verification and evaluation of agency C&A processes;
- Focus on utilizing the expertise and experience found in ACIO-CS to remedy deficiencies leading to denial of authorization;
- Standardize forms and templates and automate the documentation process to ease the manual burden of agency reporting;
- Reduce contractor costs and increase contractor efficiency by utilizing a C&A process based on NIST 800-37; and
- Improve the transparency of the C&A process by utilizing a C&A process based on NIST 800-37.

There are currently differences between the USDA C&A guidance and NIST Special Publication 800-37. These differences make this process more costly than is necessary. Because of the specialized C&A process, contractors often need more time to address process changes to meet USDA requirements. The increased time required to address learning and process changes often results in additional charges and mistakes because of process differences. A goal of the new C&A strategy is to standardize the base C&A process with NIST 800-37 and to clearly distinguish where additional USDA processes, oversight, concurrency or demands are required. Increased efficiency and clarification of expectations as well as reduced cost and time are the goals of the new C&A process.

The additional involvement of the ACIO-CS in the C&A process will provide a pool of expert resources to agencies. The ACIO-CS will be involved closely in critical areas of the C&A process for all agencies. NIST does not mandate the level of oversight USDA is requiring, but given past experiences with agency C&As, centralized expertise and assistance could be beneficial for achieving consistent authorizations to operate. Furthermore, when agencies need to remedy deficiencies, the ACIO-CS will be closely involved to ensure timely, cost-effective, and effective resolution.

The ACIO-CS will be involved in the oversight of the system categorization process, the C&A concurrency review, and the POA&M and continuous monitoring processes. During system categorization, the ACIO-CS will ensure that systems are categorized according to NIST guidance and that consistent system categorization occurs across agencies. The ACIO-CS also will ensure that similar systems have similar categorizations through a validation process. One of the largest oversight functions of the ACIO-CS will be the concurrency review, which will improve the quality, accuracy, and efficiency of the C&A process. After the initial certification package is compiled, it will be delivered to the ACIO-CS. The ACIO-CS will then review the package and render a decision or recommendations. If the decision is to deny, the ACIO-CS will become actively involved with the agency to remedy deficiencies until a favorable decision can be rendered. Systems will be monitored closely by ACIO-CS oversight personnel to ensure timely and effective deficiency resolution. When the ACIO and the certifying official agree on a C&A decision, the decision will be forwarded to the designated approving/accrediting authority (DAA).

The new C&A guide which is almost complete will serve as a standard reference for USDA C&A policy, procedures, and guidance. The vision for the new C&A policy is to provide transparent, efficient, and effective C&A with strong ACIO-CS oversight and involvement. These process changes should result in high performance information assurance in correlation with the goals of ACIO-CS and USDA.

6 Conclusion

OCIO is working efficiently and diligently to secure USDA data and information systems while making them available for everyday business. OCIO will continue to work on a comprehensive security program through projects and initiatives such as those discussed in this report. Many projects have been implemented and/or enhanced in FY 2006 to increase information systems security, promote consistent compliance and enforcement of security mandates, and create a comprehensive security management system. The information security and oversight work will continue into FY 2007 with a goal of providing even better guidance -- that also conforms to NIST policies -- for agencies.

Appendix A. Privacy Policy and Procedure Review

In order to meet the requirements of OMB Memorandum M-06-15 regarding personally identifiable information (PII), USDA will develop a comprehensive, overall Privacy Program to ensure that all privacy-related documentation (i.e., identity and number of personally identifiable information, privacy impact assessments, requests for systems of record notices, publications systems of record notices) are captured and tracked; and all required OMB and FISMA approvals, reviews and reporting requirements are identified and met.

As a first step in developing a comprehensive, department-wide privacy program, OCIO has issued a directive for USDA agencies to designate a Privacy Officer to be the primary point of contact (POC) for all privacy-related issues. The Privacy Officers will be responsible for communicating, implementing and approving a comprehensive, department-wide privacy program. OCIO is scheduling an introductory meeting with agency designated Privacy Officers to apprise of them of the action steps OCIO is taking to implement a comprehensive USDA Privacy program.

In the interim, OCIO has mandated that all employees complete the recently implemented privacy training. OCIO has also issued a data call for all agencies to identify all personally identifiable information; and provided interim guidance on complying with OMB Memorandum M-06-16 to protect Privacy and other sensitive data on agency systems.

USDA OCIO Cyber Security will take the following corrective actions to ensure the appropriate safeguards are in place to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information:

1. Identify and document Federal Privacy requirements. (See Table 4, USDA Privacy Requirements)
2. Draft process flow to address updated privacy requirements. (See Figure 12, DRAFT USDA Strawman Privacy Process)
3. Submit Privacy requirements and process flow to Privacy stakeholders for review and comment.
4. Identify/develop immediate and long term training needs in support of privacy requirements.
5. Develop Communications Plan to inform stakeholders of privacy requirements and processes
6. Develop project plan to implement new process and procedures.

USDA OCIO has completed steps 1 and 2 above, and will submit the Privacy requirements and process flow to the Privacy stakeholders (i.e., agency privacy officers, IT project leaders, agency security officers, senior agency officials, etc.) for review and comment.

OCIO will submit a high-level project plan to identify and develop immediate and long term privacy training needs; create a communication plans to keep stakeholders informed; and implement new privacy processes and procedures by October 31, 2006.

Table 4. USDA Privacy Requirements

Requirements	Source
Privacy Impact Assessments	
Privacy Impact Assessments (PIAs) are conducted for electronic systems and collections.	E-gov Act section 208, (I) (A)(1); OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (II) (C),(3)(a)(iii)
PIAs are performed whenever a System Change creates new privacy risk.	E-gov Act section 208, (II) (B)(2)
PIAs are made publicly available	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (II) (C),(3)(a)(iii)
Privacy policies are posted on agency websites	
Compliance with section 208 of E-gov Act is reported annually to OMB.	
PIAs address Privacy in the systems development lifecycle, including statement of need, functional requirements analysis, alternative analysis, feasibility analysis, benefits/cost analysis, and initial risk assessment as warranted and/or appropriate.	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (II) (C),(2)(a)(i)
The PIA document and summary (if prepared) are approved by a "reviewing official" (the agency CIO or other agency head designee) who must be someone other than the official procuring the system.	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (II) (C)(3)(a)(i)
Agencies must separately consider the need for a PIA when issuing a change to the System of Records (SOR) notice (e.g., a change in the type or category of record added to the system may warrant a PIA).	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (II) (E)(3)
PIAs are submitted to OMB.	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance
Privacy Policy on Agency Websites	
Privacy Policy Clarification. Agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (III) (A)
Content of Privacy Policies. Agencies policies must include: ▪ Consent to collection and sharing ▪ Rights under the Privacy Act	OMB M-03-22, Implementing E-Gov Act Section 208 Guidance, (III)(D)(1) (a.) and (b.)
OMB Required Reviews	
All Federal Agencies. In addition to meeting the agency requirements contained in the Act and the specific reporting and publication requirements detailed in this Appendix, the head of each agency shall ensure that the following reviews are conducted as often as specified below, and be prepared to report to the Director, OMB, the results of such reviews and the corrective action taken to resolve problems uncovered.	Appendix I to OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining Records About Individuals

Requirements	Source
Section (m) Contracts. Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees	Appendix I to OMB Circular No. A-130,(3)(a)(1)
Recordkeeping Practices. Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.	Appendix I to OMB Circular No. A-130,(3)(a)(2)
Routine Use Disclosures. Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.	Appendix I to OMB Circular No. A-130,(3)(a)(3)
Exemption of Systems of Records. Review every four years each system of records for which the agency has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.	Appendix I to OMB Circular No. A-130,(3)(a)(4)
Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.	Appendix I to OMB Circular No. A-130,(3)(a)(5)
Privacy Act Training. Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.	Appendix I to OMB Circular No. A-130,(3)(a)(6)
Violations. Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.	Appendix I to OMB Circular No. A-130,(3)(a)(7)
Systems of Records Notices. Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register (See paragraph 4c of this Appendix).	Appendix I to OMB Circular No. A-130,(3)(a)(8)
FISMA Reporting Requirements	
Demonstrate through documentation that the Privacy Officer participates in an all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy).	Annual FISMA report, Senior Agency Official for Privacy, Section D (I.), Senior Agency Official for Privacy Responsibilities, (1)
Demonstrate through documentation that the privacy officer participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under circular A-19.	Annual FISMA report, Senior Agency Official for Privacy, Section D, (I.), Senior Agency Official for Privacy Responsibilities, (2)

Requirements	Source
Demonstrate through documentation that the privacy officer participates in assessing the impact of technology on the privacy of personal information.	Annual FISMA report, Senior Agency Official for Privacy, Section D, (I.), Senior Agency Official for Privacy Responsibilities, (3)
Agency has a training program that ensures all agency personnel and contractors with access to Federal data are generally familiar with privacy laws, regulations and policies and understand the ramifications of improper access and disclosure.	Annual FISMA report, Senior Agency Official for Privacy, Section D, (II.), Procedures and Practices, (1)
Agency has a training program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities.	Annual FISMA report, Senior Agency Official for Privacy, Section D, (II.), Procedures and Practices, (2)
Agency conducts required OMB Circular A-130 reviews of activities mandated by the Privacy Act. (*see OMB required Reviews*)	Annual FISMA report, Senior Agency Official for Privacy, Section D, (II.), Procedures and Practices, (3)
OMB Reporting	
Submit PIAs as part of business cases (300) or Exhibit 53 (Annual). Due September, 30, 200n.	Per 3/20/06 meeting with Eva Kleederman, OMB Info Tech & Policy
Make Privacy Impact Assessments (PIA) available to the public (i.e., publish on agency website).	Per 3/20/06 meeting with Eva Kleederman
Submit Computer Matching Report (Biennial). Due June 30, 2006.	Per 3/20/06 meeting with Eva Kleederman

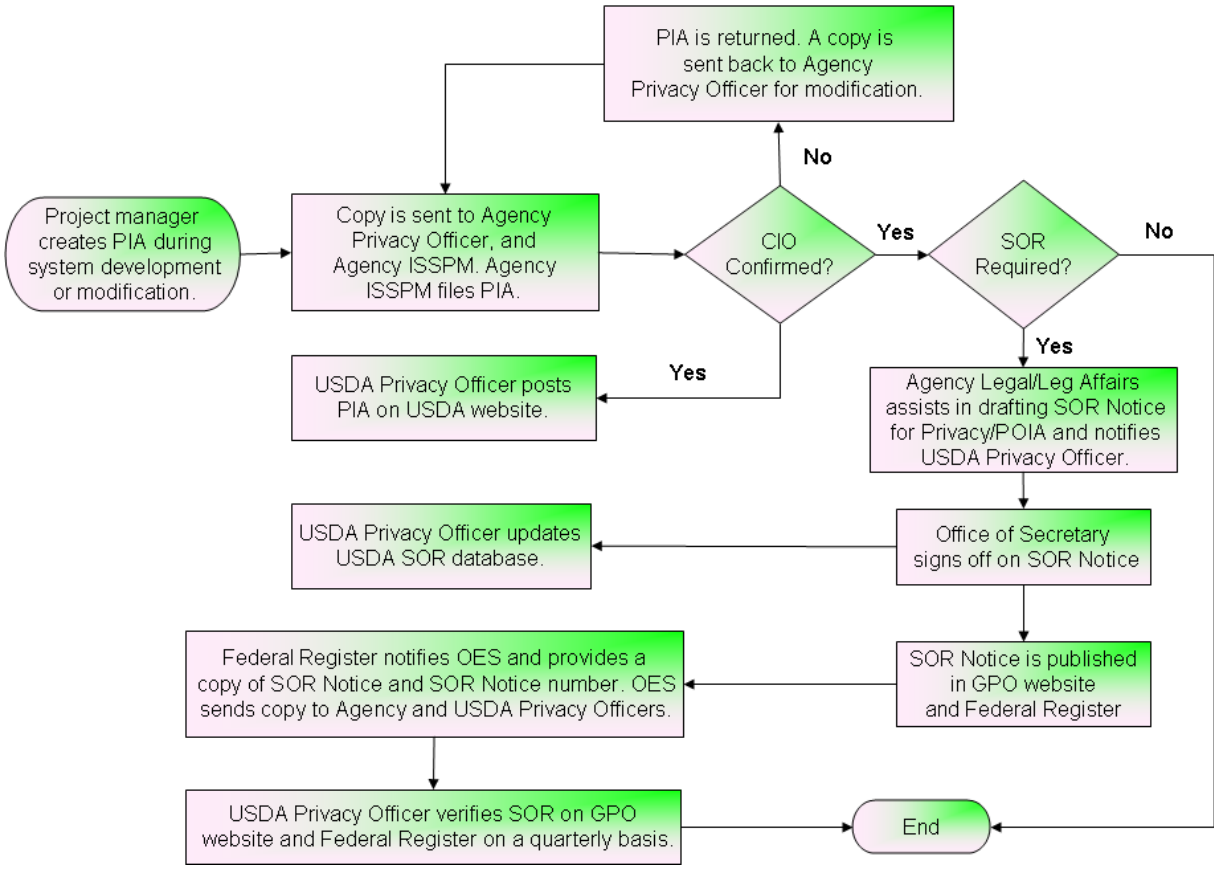


Figure 12. DRAFT USDA Strawman Privacy Process

Table 5. Privacy Deliverable Schedule

Annual	Biennial	Every Four Years
1. FISMA Report (OMB)	1. Recordkeeping Practices. Review agency recordkeeping and disposal practices.	1. Routing Use Disclosure. Review the routing use disclosure associated with each SOR to ensure the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.
2. Matching programs. Review ongoing matching programs in which the agency has participated during the year to ensure the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines are met.	2. Contracts. Review a random sample of agency contracts that provide for maintaining a SOR to ensure that the agency function is accomplished and that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees.	2. Exemption of Systems of Records. Review each SOR for which the agency has promulgated exemption rules.
	3. Privacy Act Training. Review agency training practices to ensure that all agency personnel are familiar with the requirements of the Act.	
	4. Violations. Review the actions of agency staff that resulted in either the agency being found civilly liable or an employee being found criminally liable.	
	5. Systems of Record Notices. Review each SOR notice to ensure that it accurately describes the systems of records. Where minor changes are needed, ensure that an amended notice is published in the Federal Register.	

Appendix B. Acronyms List

The acronyms used in this document are listed in alphabetical order below.

Table 6: General Acronyms

Acronym	Description
ACIO	Associate Chief Information Officer
ASSERT©	Automated Security Self-Evaluation and Remediation Tracking
ATOR	Authorization to Operate with Restrictions
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CCB	Configuration Control Board
CD	Compact Disc
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
COOP	Continuity of Operations
CPIC	Capital Planning and Investment Control
CS	Cyber Security
CSAT	Computer Security Awareness Training
CSO	Computer Security Operations
DAA	Designated Approving/Accrediting Authority
DM	Department Manual
DR	Department Regulation
EAR	Enterprise Architecture Repository
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
IDS	Intrusion Detection System
IA	Information Assurance
IP	Internet Protocol
IPS	Intrusion Prevention System
ISD	Information Security Division
ISSPM	Information Systems Security Program Manager
IT	Information Technology
IV&V	Independent Verification and Validation
LDRPS	Living Disaster Recovery and Planning System

Acronym	Description
MITS	Management Initiatives Tracking System
NIST	National Institute of Standards and Technology
NSA	National Security Administration
OMB	Office of Management and Budget
P2P	Peer-to-Peer
PED	Personal Electronic Device
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
SLC	System Life Cycle
SOC	Security Operations Center
SOP	Standard Operating Procedure
SOR	Systems of Record
SP	Special Publication
USDA	United States Department of Agriculture
UTN	Universal Telecommunications Network

Agency acronyms are defined in the following table.

Table 7: Agency Acronyms

Agency	Agency Name
AMS	Agricultural Marketing Service
APHIS	Animal and Plant Health Inspection Service
ARS	Agricultural Research Service
ASCR	Assistant Secretary, Office of Civil Rights
CR	Civil Rights
CSREES	Cooperative State Research, Education and Extension Service
DA	Departmental Administration
ERS	Economic Research Service
FAS	Foreign Agricultural Service
FNS	Food and Nutrition Service
FS	Forest Service
FSA	Farm Service Agency
FSIS	Food Safety and Inspection Service
GIPSA	Grain Inspection, Packers, and Stockyards Administration

Agency	Agency Name
NAD	National Appeals Division
NASS	National Agricultural Statistics Service
NRCS	Natural Resources Conservation Services
OBPA	Office of Budget and Program Analysis
OC	Office of Communications
OCE	Office of the Chief Economist
OCFO/FS	Office of the Chief Financial Officer – Financial Systems
OCFO/NFC	Office of the Chief Financial Officer – National Finance Center
OCIO	Office of the Chief Information Officer
OES	Office of the Executive Secretariat
OGC	Office of the General Counsel
OIG	Office of Inspector General
RD	Rural Development
RMA	Risk Management Agency