FISMA Report

Fiscal Year 2008

Date: September 30, 2008

Prepared for: Office of Management and Budget

By: The Office of the Chief Information Officer

Table of Contents

List of Figures

1 Introduction

1.1 Fiscal Year 2008 Highlights

The United States Department of Agriculture (USDA) is in the first 12 months of a 36 month program to implement a Comprehensive Security Program (CSP) that protects the assets and information of the Federal Government. Prior to CSP, the Office of the Chief Information Officer (OCIO) managed cyber security through a loose federation of agencies struggling to adapt complex policies and processes. Compliance was measured through information requests accumulated through a series of agency populated spreadsheets. With the complexity and the size of information infrastructure and systems required to support USDA's diverse programs, manual processes and a federated approach is both expensive and ineffective.

OCIO is now implementing a best practices approach used by leading corporations that emulate the size and complexity of a hundred billion dollar, diverse operating entity. This approach uses independent reviews, the reduction of computer locations, centralized tools, and multi-level monitoring to support all levels of the organization. The major items in this comprehensive program include:

1. An independent Program Reviews for Information Security Management Assistance (PRISMA) review of the current security program;

2. Adjustments in Department regulations;

3. A review and understanding of the security performed by the Universal Telecommunication Network (UTN)/Networx providers;

4. Reorganizing USDA OCIO operations to support full time employees (FTEs) for an USDA Security Operations Center (SOC);

5. Consolidating critical mission applications into data centers where environment and communication can be monitored;

6. Procuring the proper security and monitoring tools for the Department for network security, electronic asset management, desktop monitoring, and desktop application management;

7. Continuing the education of employees on the proper cyber security and privacy information skills;

8. Increased training for information technology (IT) management and IT employees on proper security techniques;

9. Improving the quality of the Certification and Accreditation (C&A) process for USDA systems;

10. Addressing and correcting system security vulnerabilities located during management's internal control reviews and audits, OCIO audits, and OIG audits;

11. Implementing Homeland Security Presidential Directive-12 (HSPD-12) for dual factor authentication and whole disk encryption on all USDA desktops, laptops, and mobile computing devices with processing capabilities;

12. Implementing E-Authentication and single sign-on for USDA applications;

13. Implementing Cyber Security Assessment and Management (CSAM) to allow for a more comprehensive security review;

14. Reducing external connections to two under the Trusted Internet Connections (TIC) program;

15. Reducing e-mail and collaboration systems from 28 to 1 system that is heavily monitored for malicious software;

16. Selection of a core application architecture and the identification of multi-agency business processes to initiate reduction in the number of applications and processes to manage application security, process controls, and logical access controls;

17. Deep dive packet analysis of incoming and outgoing communications to protect government information;

18. Penetration and source code testing for security vulnerabilities; and

19. Audit and reviewing wireless connections and agency system security by the OCIO.

With this comprehensive list, fiscal year (FY) 2008 has been a year of fast-paced changes, accomplishments and challenges for the USDA. USDA has established several councils and oversight committees to address the material weakness in IT security, and to address the complexities of the comprehensive program. USDA IT security personnel have collaborated, planned, and labored to improve IT security within the Department on a day-to-day, hour-to-hour basis.

During these difficult budget times, USDA's employees have shouldered the initiative to move these actions forward while minimizing the impact on mission programs and agencies. USDA personnel planned, analyzed, coordinated, trained and executed to make progress and accomplish their tasks better, smarter, faster, and more consistently.

The pace set to comprehensively correct this longstanding issue is impressive. Even with the challenges of stable funding streams, the employees of USDA increased their efforts to meet all milestones.

It should be noted that most of the efforts will not show visible progress in this year's Federal Information Security Management Act (FISMA) score. This year's progress of conducting

independent reviews, the acquisition of centralized security tools, and monitoring systems sets the stage for the permanent improvement on cyber security in the 36 month plan.

Some of USDA's larger or more visible achievements are highlighted below.

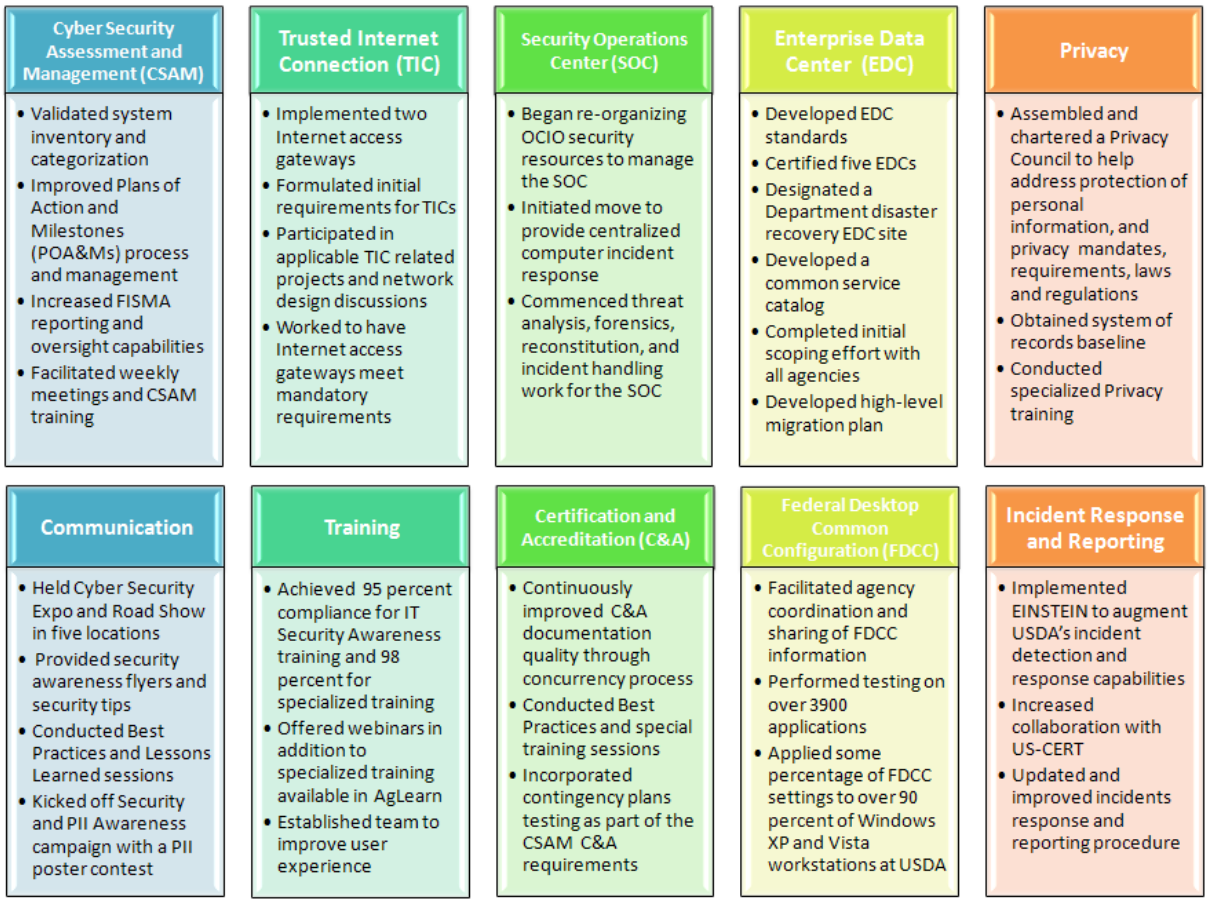


Figure 1: Highlights

1.2 New Initiatives in FY 2008

New USDA IT security oversight initiatives/activities for FY 2008 include:

- Reducing number of Trusted Internet Connections (TICs) from nine to two;
- Initiating the establishment of a Security Operation Center (SOC) to provide centralized computer incident response, and better secure USDA IT assets and information;
- Developing Enterprise Data Center (EDC) standards and certifying four USDA EDCs;
- Replacing the Automated Security Self-Evaluation and Remediation Tracking (ASSERT©) tool with CSAM as the official Federal Information Security Management Act (FISMA) reporting tool;
- Piloting PRISMA;
- Formally assembling and chartering a Privacy Council;
- Testing and implementing FDCC settings on Windows XP and Vista workstations;
- Improving and increasing Cyber Security Awareness and communications; and
- Implementing EINSTEIN to augment USDA's incident detection and response capabilities.

1.3 Background and Scope

The USDA is comprised of Departmental headquarters, 17 component agencies, and 12 staff offices with over 100,000 employees located in 7,200 offices throughout the world. Each agency has a Chief Information Officer (CIO) who oversees IT systems and processes, many of which have evolved in a federated, independent agency approach over the years. USDA is working diligently to secure IT assets and systems in accordance with best practices, Federal regulations and laws such as the Federal Information Security Management Act of 2002, which requires the CIO of each Federal Department to assess and report on the status of his or her information security program.

In FY 2008, USDA's information technology employees initiated a 36 month program to address the dire need for improvement in cyber security. This report has been prepared to highlight USDA's IT security progress and FISMA compliance in accordance with the Office of Management and Budget (OMB) Memorandum M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, and USDA internal requirements. Narratives related to security and core application systems framework are included in section 2; narratives of various reporting elements for M-08-21 are included in section 3; and narratives of Privacy and other oversight activities are included in section 4. In addition, the M-08-21, Section B – Chief Information Officer and Section D – Senior Agency Official for Privacy reports for the USDA are embedded in Appendix B; and exhibits are embedded in Appendix C.

2 Security and Core Application Systems Framework

2.1 Core Applications Systems Framework Model

Security vulnerabilities exist in a number of areas including software application and processes. In the fourth quarter of FY 2008, the Office of the Chief Financial Officer (OCFO) established a Core Application Systems Framework (CASF), which will be used as a foundation for all information technology solutions at the Department of Agriculture. This is also the foundation for the Department's Enterprise Architecture to support the customers and business requirements of the mission of USDA. By establishing a CASF, the Department's technology can be developed and integrated in the most efficient, low cost manner to provide the proper level of security and controls.

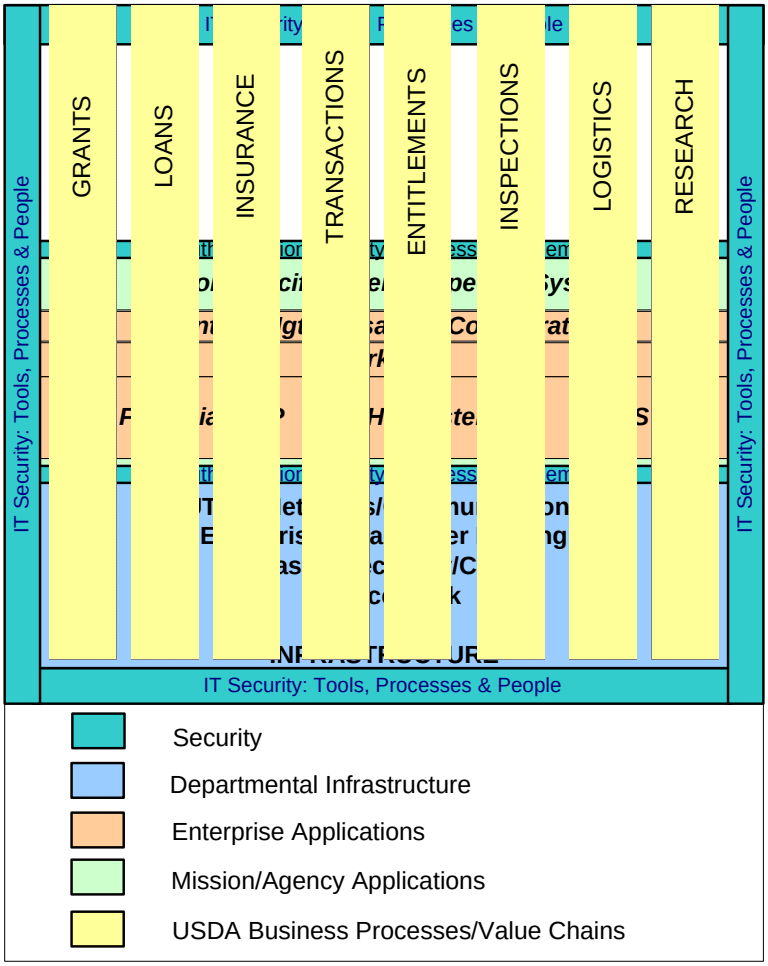


Figure 2: IT Security: Tools, Processes & People

Systems supporting the CASF will be developed and maintained to ensure that they meet all of the security and information retention requirements of the Federal Government. Commercial solutions will have all security patches applied, and will maintain no less than one version less than the vendor's current software release. Since home grown programming has over 200 different security risks, commercial software will be used when possible. If needed, home grown applications will use secure coding techniques. The systems will also be tested for 508 compliance and proper internal controls. All core systems will have penetration and source core testing completed at the Department level.

Financial systems, mixed financial systems, and the workflow system will be under the oversight of the USDA Chief Financial Officer. Since they are hosted and maintained by the National Finance Center, the human resource line of business, and human resources systems will also be under the oversight of the Chief Financial Officer. (Department Human Capital policy is managed by the Assistant Secretary of Administration.) All other CASF systems are under the oversight of the Chief Information Officer.

These systems are strategic and essential to the success of the mission areas and will be located in an Enterprise Data Center (EDC). The EDC will support the hardware architecture and the operating systems of the applications to support a low cost, environmentally friendly solution.

The following is the USDA CASF systems:

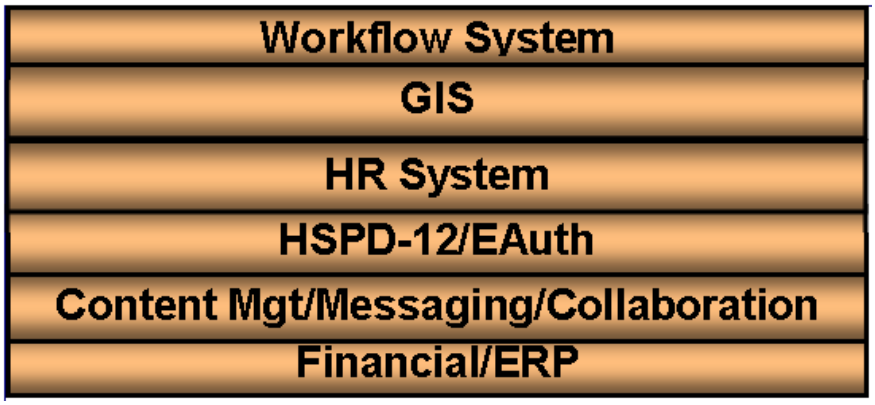


Figure 3: USDA CSAF Systems

USDA customer and business processes are designed to meet the goals and requirements of the mission areas. By combining the effort and resources of the mission areas, USDA could quickly consolidate, develop, and offer Department-wide and Government-wide processes. By reducing the number of applications USDA will have fewer applications to monitor and support. Security for these processes includes logical access controls.

The USDA Department-wide supported business processes are shown below:

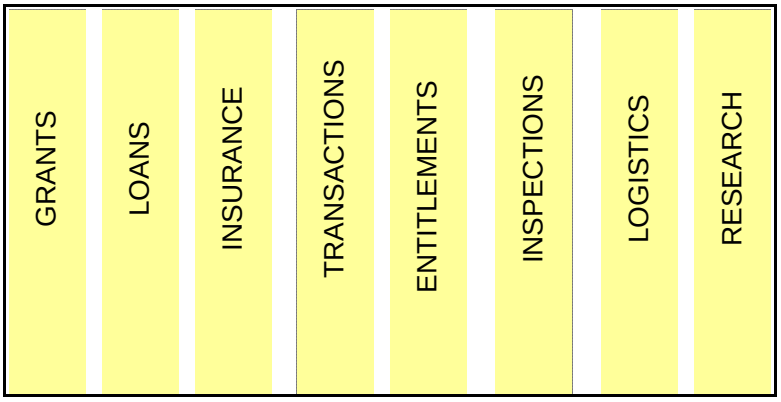


Figure 4: USDA Supported Business Processes

OCFO will have additional responsibilities to provide approval and management of the operational and control changes to the financial process. OCFO will also ensure that all financial processes meet compliance with Office of Management and Budget (OMB) Circular A-123 "Management's Responsibility for Internal Control" Appendix A "**Internal Control over Financial Reporting"** and other Federal requirements. The OCIO will have the additional responsibilities to ensure that the processes meet the requirements of enterprise architecture, Cyber Security, system refresh, and other Federal information technology requirements.

The Chief Financial Officer and the Chief Information Officer will meet together quarterly to review the fulfillment of responsibilities by the Enterprise Change Control Board (ECCB) and the individual committees.

The ECCB is established to develop and support the CASF and primary Department-wide processes. With the CASF and the Department-wide Customer Support and Mission Support Processes, the Chief Information Officer and Chief Financial Officer will be establishing a new framework for the ECCB. The ECCB includes the following system security responsibilities:

- Provide the proper operating environment for safeguarding the network system and key infrastructure of USDA.
- Provide oversight to ensure that all USDA network and systems are meeting Federal Information Security Management Act (FISMA) and other Federal information technology regulations.
- Ensure that the CASF and other mission critical systems are no less than one version older from the vendor's current release.
- Ensure that the proper controls are in place for the development, testing, and integration of hardware, applications, and homegrown code into current operating systems.

- Minimize the number of applications, systems, and processes that must be supported and monitored at USDA.
- Support a standardized FDCC workstation configuration that will provide the maximum security to the USDA network.
- Ensure that the proper communication architecture is in place for the support of Department-wide and mission specific application.
- Provide an automated solution to meet the Federal requirements for the retention and protection of electronic documents and privacy information across the Department.
- Support the proper tool for accessibility (508 compliance), mobile computing, thin client, and teleworking.

2.2 USDA OCIO Security Operations

The OCIO has taken steps to reorganize and more clearly define its security operations, security policy and compliance branches to more effectively and efficiently carry out IT security execution within the Department. This reorganization will ensure that security operations duties are distinct responsibilities that reside under the scope of control of the Deputy CIO for Security and Operations. Policy and compliance will be directed by the Deputy CIO for Policy.

Processes and procedures for both areas will be based on Information Technology Infrastructure Library body of best practices for Security. A contract was awarded in September 2008 for independent third party assessment of security processes, and will provide the foundation for process improvement implementation.

Furthermore, the USDA is carrying out an independent assessment of its current Security Operations Center (SOC) capability and will be looking for short, mid, and long-term opportunities to strengthen data collection, reporting, and threat analysis functions in this critical area. The USDA SOC will be leveraging the security tools acquisition (discussed in this FISMA report) to provide robust, timely, end-to-end monitoring of the USDA network. Creating a SOC gives USDA the capability to centrally manage and monitor the network and security systems across the Department's diverse IT environment, intelligently and proactively alert the right people at the right time about critical security events, and respond quickly and consistently to emergent threats.

The creation of the SOC will reduce risk, minimize downtime, and wage a progressively proactive defense-in-depth war against those who would obtain our data for illicit objectives. Implementing tools to report security incidents in real-time (via pagers, e-mail, or a centralized security management console) and implementing enterprise-wide Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) will harden our perimeters and improve our threat posture because of the timeliness of threat mitigation.

Finally, the establishment of the SOC will enable fast and effective incident response and recovery by implementing security information management tools to allow security events to

be grouped and annotated, and incidents to be declared and acknowledged faster. These actions will enable the security team to manage events, respond effectively, and develop comprehensive enterprise-wide corrective/preventative actions.

OCIO Security Operations will oversee and support Agency security operations to ensure that activities such as computer forensics conform to security best practices and that security tools are implemented to ensure an enterprise security posture.

As a whole the re-organization and re-alignment of security roles, responsibilities and execution of duties combined with process re-engineering and refinement will move USDA forward over an 18-24 month period directly resulting in USDA as a center of excellence for Cyber Security.

2.3 Trusted Internet Connections

OMB Directive (M-08-05) titled "Implementation of Trusted Internet Connections (TIC)" is intended to create a secure cyber defense perimeter between the Federal government and the Internet. During FY 2008, USDA staff participated in many working group sessions with OMB to develop the TIC requirements. .

2.3.1 Current TIC Requirements

USDA has two Internet Gateways. Many of the TIC requirements are currently being met under the Universal Telecommunications Network (UTN) contract. The requirements for TIC have not been completely finalized, and may change in the future. The current TIC requirements include:

- Encrypted e-mail will be scanned by an anti-virus system.
- All web traffic to and from the USDA is proxied and scanned for malignant traffic before transmission to reduce threats to USDA PCs.
- File transfer protocol (FTP) is scanned for malignant transmissions.
- IPv6 is supported.
- Site-to-site Virtual Private Networks (VPNs) must be available at the gateways to improve secure communications with external entities.
- All security log data will be retained for longer periods to improve forensic capability.
- A SOC capable of supporting information classified as Top Secret, and providing centralized computer incident response, must be established.

2.3.2 Current TIC Project Status

OMB and Department of Homeland Security (DHS) are currently coordinating TIC network design sessions that require agency network engineering support. These sessions will create the basis for the final design, and actions that need to be performed to ensure ongoing success of the TIC initiative.

OMB expects to have a draft of the final design for agency review and comment by September 30. The General Services Administration (GSA) telecommunications contract, known as Networx, will be modified to include TIC services. GSA issued a Request for Proposals to the five Networx vendors in July. Bids were accepted in late September. GSA and OMB expect to have TIC services available in November 2008.

2.3.3 TIC Related Projects

Situational Awareness and Incident Response

Situational Awareness and Incident Response (SAIR) is the security community within the Federal Government with several working groups developing a phased approach to improve the security of Federal networks and systems. This is part of the OMB Information Systems Security Line of Business (ISSLOB). SAIR addresses both Tier 1 and Tier 2 improvements. Tier 1 consists of awareness with TIC and C&A as major projects. The projects are being executed to force Federal Agencies to improve security using common methodologies by using shared services to implement these methodologies.

Other Projects

The OMB ISSLOB Project Management Office (PMO) is managing several projects. TIC, C&A, and T2T are some of these projects. The projects are phased in their execution using Tier terminology. T2T involves Tier 2 Training. This project will establish common security training requirements and training for Federal Government employees. One of the goals is to provide shared service training providers to ensure consistency in the training.

Both C&A and T2T activities, as well as future activities are important in developing the best possible solutions for providing the best security tools and services at the best price in supporting the larger goal of raising the security baseline of the Federal information enterprise.

2.4 Enterprise Data Center

2.4.1 OMB Bulletin 96-02

OMB issued Bulletin No. 96-02, *Consolidation of Agency Data Centers*, on October 4, 1995. This Bulletin called for agencies to reduce their total number of agency data centers into a smaller number of physical locations; collocate small and mid-tier computing platforms in larger data centers, modernize remaining data centers to improve delivery of services, and outsource information processing requirements to other Federal or commercial data centers if the aggregate installed base is below minimum target size.

2.4.2 Enterprise Data Centers and Critical Systems Memo

USDA released its Enterprise Data Centers and Critical Systems memo on January 4, 2008, requiring critical IT located in the US to be hosted in the Department's shared service data

centers. These critical information technology solutions include mission critical systems, mixed-financial systems, disaster support systems, incident response systems, and information systems that handle privacy, sensitive and personal identifiable information (PII).

2.4.3 Current EDC Status

USDA has addressed the first steps necessary to meet the OMB requirement for relocating all agency and staff office applications and storage network hardware to consolidated data centers, and has established a framework of requirements for security, infrastructure, service, management, and maintenance of consolidated centers hosting the USDA applications. The USDA has nearly 3,000 distributed computing sites in service centers and over 120 data rooms. This represents inflows and outflows of data that will be consolidated to five USDA Enterprise Data Centers that are built and certified with physical, cyber, and personnel security in mind. This is the same consolidation practice currently taking place across corporate America and other agencies. Besides mitigating security weaknesses, consolidation to EDCs bring about energy savings and savings from using a single set of management and monitoring tools. Currently these tools are duplicated many times over through the many distributed locations. The EDCs will also use virtualization technologies that will greatly increase the productivity of human resources as well as hardware and software productivity while decreasing the overall hardware footprint in the data centers.

The EDCs are the central location for shared computing resources and are the most concentrated, complex and strategic component of the IT environment, and therefore is the starting point for pursuing reduced complexity and better manageability. In simplifying the environment and increasing its manageability, data center consolidation offers a number of business benefits. Five areas of business benefits in data center consolidation are:

- Reduced costs (staff, facility and complexity);
- Improved security (physical, cyber, and personnel);
- Keeping up with business challenges;
- Improving service levels and availability; and
- Minimizing the impact of external pressures.

The migration to enterprise data centers will continue through 2009.

2.5 Department-wide Security Monitoring Tools

USDA has developed and awarded an enterprise security tools acquisition that will greatly enhance the Department's ability to proactively monitor its network from end-to-end, and more quickly respond to IT security threats. Implementation of the tools selected under this acquisition will provide the Department with a standard set of tools across all agencies that will allow for centralized monitoring and reporting of inventory, file and application management, data loss prevention, vulnerability scanning and penetration testing. The

security tools acquisition covered more than 200 discrete requirements in the 5 key categories listed below:

1. Asset Management for Security
   - Asset Discovery / Asset Management
   - Patch Management
2. Network Access/Admission Control
3. Internal Intrusion Detection
4. PII Data Monitoring, Protection and Loss Prevention
   - Discovery
   - Leakage and Audit Monitoring
   - Alerting
   - Theft Prevention
   - Peripheral Device Control (Physical access)
   - Compliance with OMB Circular No. A-123 Appendix A
   - Source/Executable Code Analysis of Application Security
   - FDCC Compliance Using the SCAP Protocol
5. Vulnerability Code Scanning
   - Analyze the source code for vulnerabilities that could potentially be exploited.
   - Support all major languages such as C/C++, Java, .NET, etc.
   - Ability to scan large code bases and complex enterprise applications in a rapid and comprehensive manner.

Purchases at the end of FY 2008 will have immediate results in the first two quarters of FY 2009. USDA has selected one toolset that will cover more than 150 requirements, providing an enterprise-wide capability for asset discovery, asset management, patch management, and theft prevention. This initial capability will also be coupled with the purchase of a toolset for vulnerability code scanning.

Vulnerability code scanning refers to the scanning of the underlying software that makes up an application or system. Traditionally organizations have focused on protecting and securing the perimeter of a network. Vulnerability code scanning provides another layer of defense that looks deep within applications to ensure that they are built securely from inception. In addition, USDA is reviewing products to allow for scanning of web based applications to ensure that they are not vulnerable to attack.

The sum of these implementations will cover all of the 200 requirements and provide the basis for a more robust defense in-depth security posture that will better secure USDA systems and networks. Improved asset management, perimeter defense, penetration testing and vulnerability code scanning will make USDA a much more difficult target for those intent on attacking US Government systems.

2.6 Collaborative Web Technologies

USDA uses Microsoft Windows SharePoint and other webinar tools for collaborative sharing of information and training. The usage of these technologies is relatively new to USDA, and is being piloted. Department policies on access control, internet controls and applications (e.g., DM 3525-001, DR 3180 Appendix O) are followed for the usage of these web tools.

2.6.1 Microsoft Windows E-mail and SharePoint

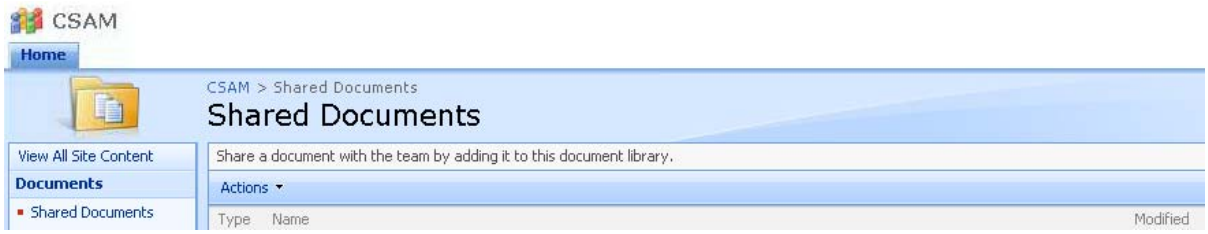


Figure 5: Sample SharePoint Site

The Department currently has 3 different e-mail types and 29 different e-mail locations. E-mails sent and received both within USDA and to the outside transfer more malware than any other system at USDA. USDA is moving all agencies to a centrally managed e-mail system. The system will incorporate the most sophisticated tools to provide deep packet security monitoring of information entering USDA. During the early FY 2009 conversion, USDA will not be transferring the history from the old e-mail system due to known and unknown malware in the agencies systems.

Microsoft Windows SharePoint is a collaborative web tool, which can be used to help teams stay connected, provide content and records management, and supply access to information. USDA has leveraged SharePoint in FY 2008 to improve collaboration and information delivery for various groups including those on the Office of Inspector General (OIG), FISMA, Privacy Council, FDCC and CSAM teams.

In addition, the use of collaboration sites to store information reduces amount of e-mails and e-mail attachments. E-mail attachments are the number one distributor of malware at USDA. With the proper use of the collaboration tools and the oversight of the systems in the USDA data centers, the implementation of Department-wide collaboration tools will reduce cyber incidents.

2.6.2 Webinars

USDA uses a commercially available Web conferencing tool, which allows USDA to provide on-the-fly or scheduled presentations, perform live demonstrations, collaborate and conduct training. The vendor of the Web conferencing tool has touted its product to be private and secure, using built-in, always-on security measures to protect user privacy and access to data and computers. It is an online meeting solution that uses end-to-end 128-bit Advanced Encryption Standard (AES) encryption for all meeting data, which includes screen images, files, keyboard and mouse input and chat text. According to the vendor site, it is not possible to catch or spread a virus, or become exposed to spyware when using its product as either a host or attendee since its product's screen-sharing technology preserves the secure barrier between systems.

USDA has been using webinars in FY 2008 to train personnel and conduct meetings. This tool has allowed USDA personnel greater flexibility for collaborating regardless of physical location, and reduced traveling costs. Trainings and meetings for CSAM, for instance, are conducted each week using webinars.

3 M-08-21 Related Oversight Activities

3.1 FISMA Systems Inventory and CSAM

After review, USDA found that its diverse and complex structure required comprehensive tools to manage and address system documentation, inventory, correction plans, and general security issues. After analyzing the approved government tools, the agencies agreed to purchase and migrate to the CSAM comprehensive FISMA compliance tool developed by the Department of Justice (DoJ). This tool provides the ability to identify threats and vulnerabilities through the use of embedded National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems. Using CSAM, IT security standards and procedures can be tailored to meet FISMA reporting requirements, provide complete Plans of Action and Milestones (POA&Ms) tracking and management, and support the implementation of a repeatable process that continually assesses control effectiveness.

CSAM features allow for greater efficiency in the management of cyber security. While the CSAM system is more expensive than the previous ASSERT© system, over time, the comprehensive tool will provide for a lower operational cost and better cyber security management associated with Certification and Accreditation (C&A) document development and maintenance, POA&Ms management, IT inventory management, FISMA reporting and controls, and other government requirements.

The USDA agencies engaged with OCIO cyber security to implement the CSAM system in record time. To implement the system, an Integration Program Team (IPT) was assembled to develop and coordinate guidance to effectively use, deploy and integrate CSAM within USDA. The IPT is responsible for coordinating all aspects of the planning and monitoring processes.

3.1.1 System Inventory Validation

USDA completed a comprehensive validation effort to align its FISMA systems to system and subsystem records maintained in the Investment and Enterprise Architecture (EA) Repositories. The validation effort was facilitated by establishing unique identifiers that simplify the ability to cross reference records across multiple repositories. The results of this effort enable USDA to relate EA, Investment, and Security data across repositories.

3.1.2 POA&M Management Focus

The CSAM implementers in FY 2008 focused on converting ASSERT© information into CSAM, and training agencies on rudimentary use. As part of the process, some default CSAM settings were used. USDA is aware of these issues, and will continue to monitor and address them. In the meantime, USDA will continue to improve upon its POA&M process through its Executive Steering Committee (ESC), which reviews and analyzes POA&Ms across the

Department to determine areas of synergy and high risk, and address them with agencies on almost a weekly basis.

3.1.3 POA&M Management Process Progress

In general, ASSERT© POA&M management capabilities were inadequate, lacking the ability for instance to prioritize or lock down due dates. Since the ASSERT© tool was used for about eight months, and CSAM for about four months of the fiscal year, the converted information will reflect these inadequacies. CSAM work will continue to improve upon the ASSERT© converted information and process to provide better controls for POA&M management. The POA&M management process in FY 2009 will also include the risk based prioritization

3.1.4 System Categorization Re-Performed

Figure 6: Screen Capture from CSAM Training

Converting ASSERT© data into CSAM has been a major undertaking in FY 2008. OCIO's focus with the agencies on validating and updating system inventory in FY 2007 and FY 2008 has played an important role in the success of the project. During the CSAM conversion, agencies have re-performed/validated the accuracy of system categorizations. This allows the agencies to focus on the proper controls from the NIST 800-53 guidance during Certification and Accreditation efforts, improving the effectiveness of continuous monitoring processes.

3.1.5 Integration of FISMA and Other Requirements

OCIO and OCFO worked together to address the longstanding information technology weakness. In FY 2008 OCIO and OCFO jointly expanded the scope of the Department's A-123, Management's Responsibility for Internal Control testing program to evaluate the effectiveness of 800-53. Jointly, the two offices identified the key core controls necessary to facilitate compliance with the Federal Managers Financial Integrity Act of 1982 (FMFIA), Federal Financial Management Improvement Act of 1996 (FFMIA), FISMA, and A-123 Appendix A requirements. Currently, 91 percent of USDA systems have had security controls tested and reviewed. Upon completion of the testing, the USDA agencies and offices were required to identify control vulnerabilities and create Plan of Action & Milestones (POA&Ms) as part of FISMA requirements and assessment processes in CSAM. In FY 2009 the USDA

will utilize CSAM as the repository for all information technology controls documentation. USDA agencies and offices are required to conduct tests, document status, identify weaknesses and create POA&Ms as part of FISMA requirements and assessment processes in CSAM.

3.2 C&A and Security Controls and Contingency Plan Testing

3.2.1 Concurrency Reviews

Figure 7: Sample Concurrency Review Slides

3.2.1.1 Improvements in Concurrency Review Process

USDA has expended considerable resources and energy into improving its C&A process in FY 2008. The concurrency review, for instance, is designed to increase oversight and improve the quality, accuracy and efficiency of the C&A process. The concurrency review process in FY 2007 was focused on meeting minimum IT security requirements, since there were many packages to review in a very short timeframe. The focus in FY 2008 is on improving the quality of C&A documentation submitted to identify and correct root causes of non-compliance. To accomplish this, USDA has:

6. Improved C&A templates to ensure NIST requirements are addressed;
7. Updated checklists to provide better details for C&A package deficiencies noted;
8. Conducted two Best Practices and four special training sessions on the concurrency review process, C&A requirements, agency weaknesses and remediation strategies;
9. Incorporated testing of contingency plans as part of CSAM requirements;
10. Verified Privacy Impact Assessments (PIAs) and system categorization;
11. Identified sustainable internal control processes to implement into CSAM;
12. Worked to increase senior management attention and involvement;
13. Maintained and regularly updated a master C&A tracking spreadsheet (MCATS) to track date of last accreditation, and accreditation due dates for the next few fiscal year cycles;
14. Verified that POA&Ms are created in CSAM to address and track deficiencies noted; and
15. Continued to report on C&A progress and status in the Weekly Activities Report (WAR).

3.2.1.2 Effectiveness of Concurrency Review Process

The USDA concurrency process has been evolving, identifying more weaknesses and providing more substantive analyses of C&A packages over prior years' processes. This stringent process has been very successful in identifying and addressing weaknesses. During FY 2008, reviewers have even worked with agencies individually to improve agency C&A documentation and mitigate weaknesses. In some instances, agencies were allowed to obtain authorizations to operate (ATOs) with the condition that POA&Ms are created to address deficiencies noted in concurrency reviews. Currently, over 90 percent of all USDA agency and contractor systems have been certified and accredited, but only about a third of all systems have undergone the improved concurrency process of FY 2008. Agencies are finalizing the remaining 10 percent of system C&A packages for accreditation, and all systems are expected to undergo the improved concurrency review process of FY 2008 in the next two years as part of the C&A review cycle.

3.2.2 Contingency Plan Testing

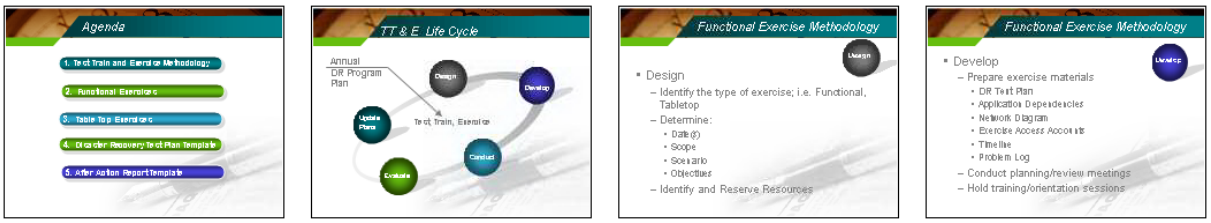


Figure 8: Sample Disaster Recovery Best Practices Slides

Various improvements have been made to the contingency planning and disaster recovery process in FY 2008. These include reworking the IT Contingency Plan (ITCP) template, the Disaster Recovery Plan (DRP) template, the Test-Exercise Plan and After-Action Report templates, and the contingency self assessment and concurrency checklists; and revising the Contingency policy with input from various agencies and offices as part of the Contingency Planning Work Group (CPWG) activities. In addition, USDA has conducted a Best Practices session on contingency planning and disaster recovery testing with sample documentation and explanations of various types of testing. Currently, over 84 percent of the FY 2008 contingency plans have been tested.

As of September 19, per memo from Christopher L. Smith to Agency Chief Information Officers, the Enterprise Contingency Planning Program (ECPP)/ Living Disaster Recovery and Planning System (LDRPS) at USDA will be retired effective December 31, 2008. Effective September 19, 2008, CSAM will be used as the official repository for all contingency, disaster recovery and business resumption plans for each system. The retirement date of December 31, 2008 was decided upon to give agencies using the full functionality of ECPP time to migrate their plans.

3.3 Incident Detection, Monitoring and Response Capabilities

3.3.1 Incidents Growth

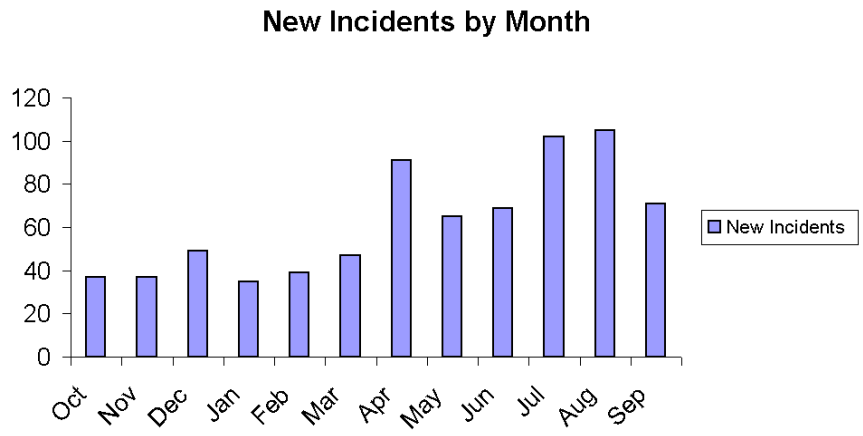


Figure 9: Number of New Incidents in FY 2008

Incidents and incidents reporting have increased 23 fold since 2006. Few incidents were reported and addressed in the years before 2006, and one person could handle and track the 30 or so incidents that were reported to Cyber Security (CS) each year. Today, due to heightened awareness, sophisticated systems and interconnectivity, attacks are detected and reported more frequently and handled in as near real time as possible. This dramatic increase has placed a huge burden on the two staff members working on incident response for the better part of FY 2008.

USDA's networks are defending against over 40,000 attempts daily to place viruses or malicious software (malware) onto its network. While this defense blocks a large amount of malware, some of the attempts use highly sophisticated malware, which is specifically designed to avoid specific tools. Once detected, USDA provides these variants of malware to the virus software providers for creating publicly distributed commercial protection.

The new detection capabilities, massive increase in attempts, and highly sophisticated nature of the malware, have resulted in an estimated average of 60 incidents each month. Incident response has become a full time effort for a team of personnel, many of whom have been recently hired. These staff members work diligently to process incidents in a timely manner, and evaluate information as they receive them to properly categorize events and incidents, and address them appropriately. While USDA continues to reprioritize its limited technology budgets to focus on this escalating issue, the Department and its agencies will struggle to manage or reduce incidents until all tools and processes are in place under the 36 month plan.

3.3.2 Implementation of US CERT's EINSTEIN

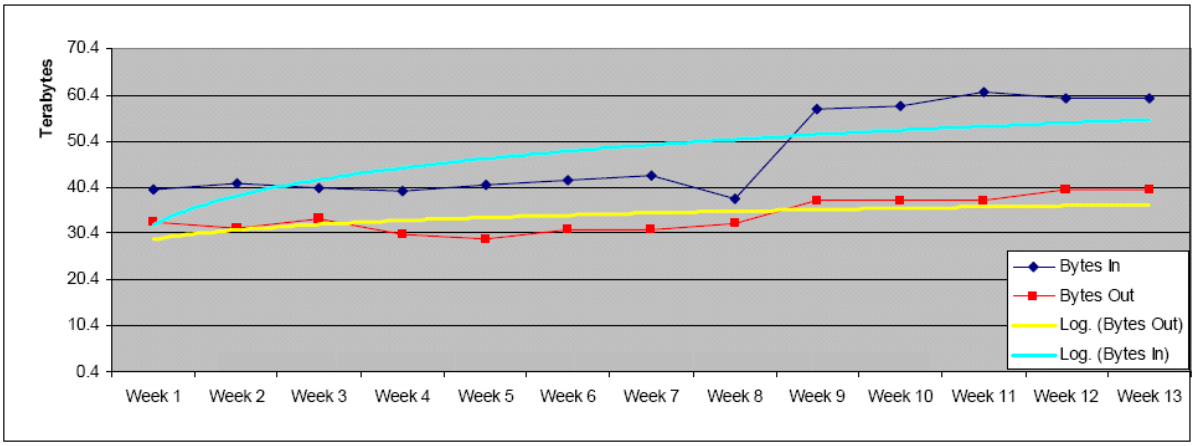


Figure 10: Total Traffic Volumes by Week During FY 2008, Q3[1]

USDA began to work with United States Computer Emergency Readiness Team (US-CERT) proactively in July 2007 to implement EINSTEIN. In response to USDA's request and OMB Memorandum M-08-05, US-CERT completed its installation of EINSTEIN sniffers into the USDA network in June 2008. This installation has augmented both US-CERT's and USDA's incident detection and response capabilities. US-CERT forwards the EINSTEIN captures of suspicious activities on the internal network along with other key information. This has resulted in an estimated 30 percent increase in the number of incidents being reported, as well as increased awareness, collaboration and involvement within USDA, its agencies, staff offices, and senior management in addressing incidents. As a result USDA has an enhanced view of internal vulnerabilities, and can better identify areas for improvement as well as areas of non-compliance. This has led to changes in incident notification, oversight and reporting procedures, which are continuing to evolve and improve.

[1] Extracted from *US-CERT Trends & Analysis Report for Fiscal Year 2008 Third Quarter (FY08 Q3) for the US Department of Agriculture*

3.3.3 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) is a protocol often used to transfer files across external networks. P2P can be used to enter unauthorized or illegal software into the USDA network. This software can be laden with malicious code or code that conflicts with critical USDA systems. The use of P2P software is prohibited on all USDA equipment and networks without explicit authorization. P2P transfers are tracked and reported on the Department's weekly activity reports.

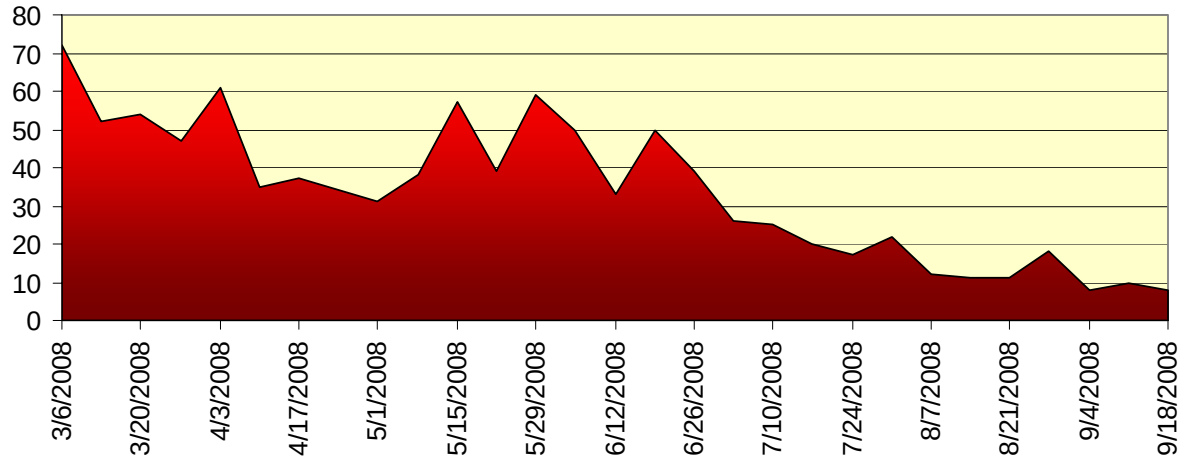


Figure 11: P2P Transfers

In early 2008, the Department met with agencies on P2P issues as well as other information technology issues. This information is tracked and reported on the Weekly Activity Report and normally distributed to the individual agencies. In FY 2008, OCIO Cyber Security focused on the implementation of EINSTEIN and several other items. During this implementation, the OCIO Cyber Security team missed a couple of periods of distributing the reports to the agencies. USDA has added incident handlers, and is aggressively addressing P2P findings, coordinating with agencies to reduce P2P traffic, and ensuring agencies obtain waivers for legitimate P2P traffic identified each week. As noted in the graph above, the success of this work is apparent in the reduction of P2P incidents by 86%.

Security Awareness Training

3.3.4 IT Security Awareness and Privacy Basics Training

Figure 12: Sample IT Security Awareness and Privacy Basics Training Slides

USDA spends considerable effort, resources and funds to provide IT Security Awareness and Privacy Basics training for all employees, contractors and partners, some of whom have limited or no computer access, and require training via CD or paper-based formats.

USDA estimates that the cost of employee time and other expenses for the training exceeds $12 million per year. The final measurement to determine the total number of employees trained is input and calculated in AgLearn, the Department's Learning Management Service. Since the course is required for computer usage in the Federal Government, agency CIOs were required to lock the password of employees who did not comply with the training requirement.

Agencies at the Department that have a large temporary or geographically dispersed workforce continue to struggle with the mandated training requirement. This year, USDA experimented with different methods to teach the training including live teaching sessions, on-line via AgLearn, CD, and paper. During FY 2008, the Office of the Chief Information Officer also reviewed the various approved federal courses to find best-in-class for the upcoming year. For FY 2009, USDA has selected the security and privacy course used at the Department of Defense.

USDA reports Department security training compliance throughout the year. In FY 2008, the USDA final calculation for compliance is 95 percent for IT Security Awareness and Privacy Basics training.

3.3.5 Specialized Training

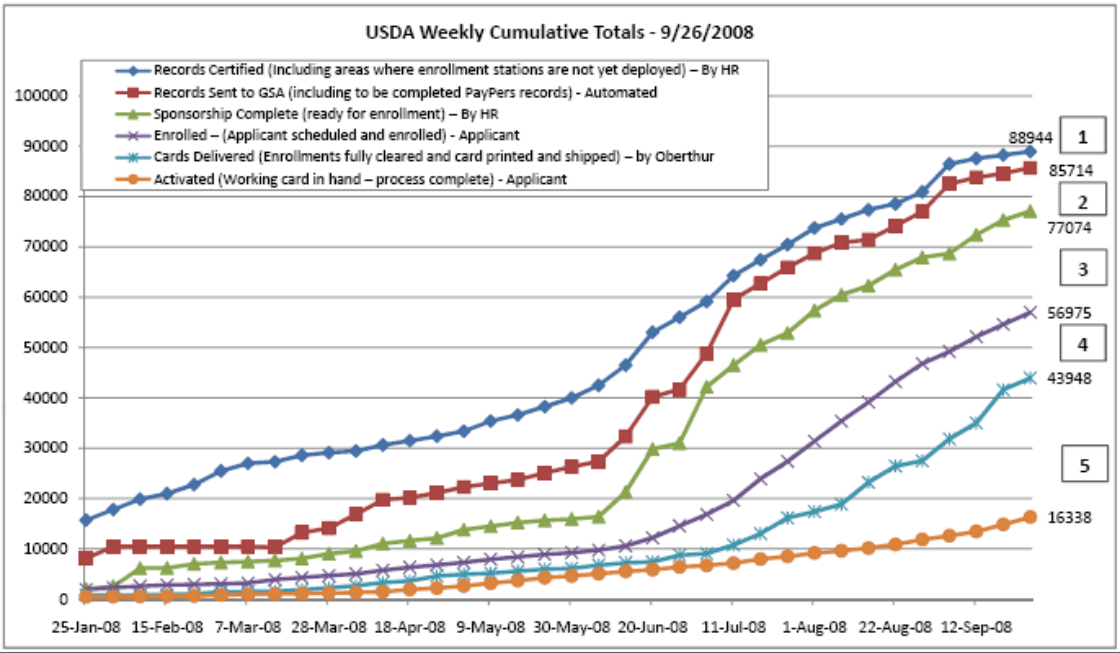
Information technology training is met using multiple venues and methods. The most comprehensive training program at USDA is the Department's on-line learning system, AgLearn. In FY 2009, AgLearn has been enhanced to include several thousand information technology courses. The courses are open to all USDA employees, at all levels of the organization, and at all locations. AgLearn includes courses that lead to highly recognized

security certifications. AgLearn has begun interactive training (webinars) in subjects including:

- Securing Your Oracle Database;
- VoIP Security and Unified Communications;
- USDA Internal Control Boot Camp; and
- Privacy Act / SORN.

3.4 Identity and Access Management Controls

USDA is well underway towards implementing a comprehensive identity and access management (IAM) controls program. There are several key initiatives encompassed under IAM including LincPass and USDA's implementation of HSPD-12. Other initiatives that will be integrated under IAM include E-Authentication, Employee Identify Management, and Non-Employee Identity Management systems. LincPass is being implemented to support both employees and contractors.



Gaps	Between	Explanation
1	Certified and Sent to GSA	Gap will close as more stations are deployed and a greater number of records certified can be sent to GSA.
2	Sent to GSA and Sponsored	Gap will close as more stations are deployed so Payroll Personnel Agencies can complete sponsorship of records.
3	Sponsored and Enrolled	Applicants may not have received enrollment email or may not have scheduled to enroll.
4	Enrolled and Cards Delivered	Records may have been flagged for Security Officer review and need to be cleared. Adjudication results of fingerprints may not have been entered.
5	Cards delivered and activated.	Applicants may not have received activation email or may not have scheduled to activate.

Figure 13: LincPass Status 9/26/2008

LincPass will be used to manage and administer both logical access to workstations, networks and systems, and physical access to facilities and buildings. Under LincPass, authentication can be based on **what you know**, such as a password or a PIN; **what you have**, such as a LincPass; or **what you are**, such as biometric data (like a fingerprint). "Two-factor authentication" means using a two of these authentication methods (**LincPass + PIN**) to increase the assurance that you are authorized to access USDA systems. USDA is implementing two-factor authentication for laptops first because of the inherent security risks in mobile computers, to make it more difficult for unauthorized persons to use a "found" laptop to access USDA systems. LincPass is being integrated with the disk encryption solutions to provide single sign-on capability to the workstations.

3.5 Whole Disk Encryption

On June 23, 2006, the Office of Management and Budget (OMB) issued Memorandum 06-16 (M-06-16), Protection of Sensitive Agency Information. The memo recommends that all agencies "encrypt all data on mobile computers/devices." Based on this memorandum, USDA established a single encryption software standard across USDA. The Whole Disk Encryption (WDE) project was initiated in August of 2007 to meet this requirement.

The USDA Whole Disk Encryption project provides encryption for computing devices for approximately 180,000 users, with up to five end-point devices each to be encrypted, for a possible total of 900,000 encrypted devices. These include laptops, desktop computers, and mobile devices with processing capabilities.

The WDE project provides a large return for the USDA – protection of all Sensitive Information at every level. The benefits of the solution provided by the WDE project include:

- Meets FIPS 140-2 compliance requirements;
- Protects "data at rest";
- Supports mobile and removable media;
- Provides centralized encryption software administration;
- Operates on a variety of operating systems;
- Supports Public-Key Cryptography Standards (PKCS) #11 USB Tokens and Smart Card integration;
- Integrates with Microsoft Active Directory; and
- Scales from small, centralized environments to large, decentralized environments.

The fully configured hardware and software environment has been delivered, as well as training for approximately fifty Agency Administrators and two-hundred agency Helpdesk Support Staff. The Pilot was completed on December 31, 2007. Encryption of all 54,000 USDA laptops is expected to be complete by December 31, 2008.

3.6 Configuration Management

3.6.1 Configuration Guides

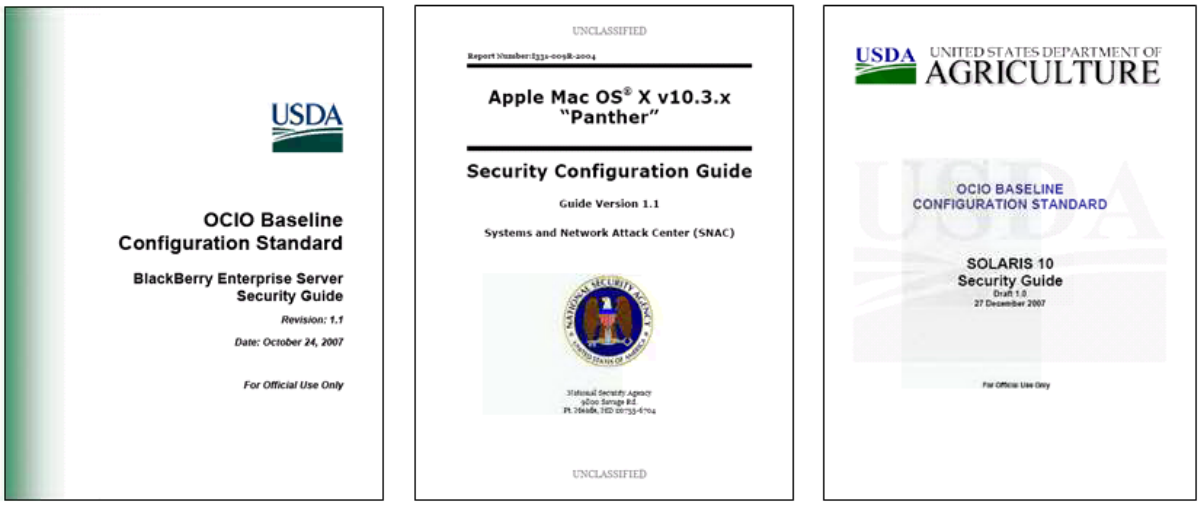


Figure 14: Configuration Guides

USDA published a number of configuration guides in FY 2008 for Apple, Mac, Windows Mobile, Cisco Switches, Blackberry Enterprise Server, Red Hat Linux Enterprise 4, etc. OCIO requires that all agencies use these configuration guides for their minimum baseline configuration in its February 14, 2008, *USDA Configuration Guides*, memo. Any exceptions to the baseline configuration must be submitted to Cyber Security for approval.

3.6.2 Federal Desktop Common Configuration

3.6.2.1 Agency Coordination

In March 2007, OMB required the deployment of FDCC to all systems that employ Windows XP and Windows Vista. To ensure compliance with OMB 07-11 and 07-18 requirements, the USDA assigned a FDCC lead to direct agency/staff office coordination; provide Departmental updates; and facilitate consolidated communications to OMB, NIST, vendors and other entities as required. An FDCC working group was established with security and technical representatives from USDA agencies and offices. The working group meets on a weekly basis to discuss progress; share solutions on testing, tools and workarounds; and help each other overcome issues such as Federal Information Processing Standard (FIPS) 140 requirements and developers' environments to achieve full compliance. An intranet web area and a SharePoint site have been set up to help document meeting discussions, provide updates on applications testing, and share group findings.

3.6.2.2 Application Testing and Reporting

The FDCC working group monitors testing status for over 5000 business (e.g., Integrated Acquisition System) and technical (e.g., HP OpenView) applications. The results are compiled into a weekly report submitted to the CIO. To date, over 60% of the applications have been tested. Home grown solutions and out-dated commercial applications are frequently incompatible with FDCC, and require complex remediation. To date, seven agency/offices have met all the testing requirements of FDCC. USDA will continue to test FDCC settings with its mission critical applications, and implement those FDCC settings.

USDA has started implementing FDCC on workstations. USDA has an inventory of over 102,000 Windows XP and Windows Vista workstations, which are required to be 100 percent FDCC compliant. Of the 102,000+ workstations, 91 percent have 50 to 100 percent of the FDCC settings applied. The remaining workstations have 10 percent or fewer of the FDCC settings applied. By December 2008, USDA expects all but one agency to meet full FDCC compliance. The remaining agency, Forest Service, requires new workstation purchases and updating software to meet the requirement.

3.6.3 Incident Reporting

Statistics of personal identifiable information (PII) and non-PII incidents are reported each week in the weekly report. USDA monitors and provides regulatory compliance guidance to agency Information Systems Security Program Managers (ISSPMs) on their incident response processes. USDA interfaces with US-CERT to provide agencies with external data captures for exploits such as ASPROX, DNS Cache Poisoning, Blackberry vulnerabilities, new Trojans, phishing, SPAM, etc. OCIO Cyber Security is working with USDA agencies and offices to limit IT administrative rights and privileges; reduce peer-to-peer (P2P) incidents; confirm scanning and patching are performed timely and properly; ensure auditing is turned on; verify monitoring and reviewing of logs; and validate configurations such as Domain Name System Security (DNSSEC) are securely implemented and in compliance with USDA and Federal policies. USDA agencies and staff offices are continuously collaborating to share ideas to minimizing the number of incidents, especially those involving equipment losses, and to improve the incident response process.

3.6.4 Updated Incident Handling Procedures

Cyber Security has updated its Security Computer Incident Response Team (CIRT) Standard Operating Procedure (SOP) several times this fiscal year in response to incidents and changes to the incident handling process. The USDA CIRT SOP has been modified in the third quarter of FY 2008 to include checklists; additional/revised PII information on forms and checklists; updated workflow diagrams and decision trees; and additional phishing and SPAM guidance.

3.6.5 Executive Review Team

USDA takes its responsibility to protect PII and sensitive data seriously, and has assembled an Incident Response Core Group (IRCG) consisting of CIO/CFO, Deputy CIO/CFO, Assistant Secretary for Administration, Senior Advisor to the Secretary, ACIO-CS, Agency CIOs, Agency ISSPMs, and USDA CIRT. The CIRT initiates the Incident Notification Plan, and takes action in response to PII incidents and/or identify theft related data breaches. In FY 2008 the IRCG group became active, meeting, reviewing and closing PII cases.

The IRCG has greatly enhanced the entire PII handling and reporting process. The group facilitated processes that enable USDA to analyze risk, respond promptly, and manage suspected or confirmed breaches. It implemented a high level course of action for notifications and responses. The Incident Notification Plan is currently being updated, and an USDA-wide PII Awareness campaign is being executed as a result of the IRCG's influence.

3.7 New Technologies and Emerging Threats

3.7.1 Overview

Figure 15: Sample Microsoft Security Bulletin Information Issued

USDA updated its policies and/or procedures on wireless, phishing and other new technologies and/or emerging threats in FY 2008. In addition, USDA is continuously monitoring its network and interfacing with US-CERT to provide its agencies and offices with the most up-to-date data captures and exploits information. Some of the FY 2008 information issued includes:

- Microsoft Security Bulletins – USDA provides its incident handling community with information on monthly Microsoft security bulletins. The information normally includes a summary of updates/resolutions for vulnerabilities and affected software.
- ASPROX Worm – USDA worked with US-CERT to provide agencies with updated information and data captures for the ASPROX worm. CS provided all agencies with step-by-step guidance on actions needed to detect, recover, report and close ASPROX incidents.
- DNS Cache Poisoning – USDA disseminated information to its agencies on the DNS cache poisoning vulnerability, and provided an update to all CIOs as well as reporting guidelines. Agencies have been asked to provide an update on the status of their patching and USDA has reported this to US-CERT. USDA participated in the US-CERT meeting

for all agencies on this vulnerability, and distributed available information, including a whitepaper on DNS cache poisoning, to agencies.

- New Trojan – USDA notified its agencies of a new Trojan at its gateways, and provided information on the Trojan files as well as a reminder to make sure all antivirus has been updated to the latest version.
- Situational Awareness Report (SAR) – USDA disseminated SAR updates as they become available, and has requested updates from its agencies (e.g., Blackberry, Microsoft Snapshot Viewer) to report back to US-CERT.

3.7.2 Wireless Oversight

In response to OIG and other wireless findings, USDA issued Departmental memos, reviewed past Departmental notices, drafted a standard operating procedure for wireless reviews, updated the wireless policy incorporating all applicable notices and memos, and required wireless access point (WAP) scanning as part of the monthly network scanning and patching performed. In addition, USDA performed wireless survey and reviews as part of its oversight activities in FY 2008.

3.7.2.1 Wireless Survey

A wireless data call/survey was sent out in November 2007 asking for number of WAPs, name, service set identifiers (SSIDs), encryption method, etc. USDA is using the information obtained from the survey to help verify its wireless inventory and perform reviews.

3.7.2.2 Wireless Reviews

USDA conducted wireless reviews on agencies, emphasizing four primary areas:

- Accurate accounting of WAPs has been performed.
- Encryption is used at the access points.
- System Security Plans (SSPs) are up-to-date with respect to wireless implementations.
- Wireless points are physically protected and monitored for intrusion.

USDA conducted wireless reviews on two agencies in FY 2008, and is planning to conduct a review in the South and Whitten buildings, which will encompass several agencies. In addition, wireless is also reviewed as part of PRISMA and security reviews.

3.7.2.3 Wireless and CSAM

CSAM has functionalities to identify steps, track information, and produce reports for wireless controls and testing. USDA will take advantage of CSAM functionalities, and track full testing of WAP security controls for the FY 2009 self assessment cycle.

3.8 Performance Metrics for Security Policies and Procedures

Agency	Systems Inventory (due 12/31/07)	Certification & Accreditation	Plans of Actions & Milestones (monthly)	Contingency Planning	Monthly Scanning	Monthly Patching	Security Awareness Training (due 3/31/08)	Privacy Basics Training (due 3/31/08)
AMS	✓	✓	N/A		Q	99%	98%	98%
APHIS	✓	RNM	✓		✓	63%	97%	97%
ARS	✓	N/A	✓		Q	✓	93%	93%
ASCR	✓	N/A	✓		✓	✓	✓	✓
CSREES	✓	RNM	✓		✓	✓	95%	95%
DA	✓	RNM	✓		Q	✓	✓	✓
ERS	✓	RNM	N/A		✓	✓	91%	91%
FAS	✓	✓	✓		Q	99%	97%	97%
FNS	✓	FR	✓		✓	✓	✓	✓
FS	✓	RNM	✓		Q	89%	95%	94%
FSA	✓	✓	✓		✓	98%	94%	94%
FSIS	✓	RNM	✓		28%	99%	91%	90%
GIPSA	✓	N/A	N/A		Q	✓	98%	98%
NAD	✓	RNM	N/A		✓	✓	97%	96%
NASS	✓	RNM	✓		✓	✓	✓	✓
NRCS	✓	RNM	✓		✓	97%	95%	95%
OBPA	✓	N/A	N/A		✓	✓	✓	✓
OC	✓	RNM	N/A		✓	98%	99%	✓
OCE	✓	FR	N/A		✓	✓	✓	✓
OCFO-FS	✓	N/A	✓		✓	✓	See NFC score	See NFC score
OCFO-NFC	✓	N/A	✓		✓	✓	✓	✓
OCIO	✓	FR	✓		✓	97%	✓	✓
OES	N/A	N/A	N/A		N/A	N/A	94%	92%
OGC	✓	N/A	N/A		94%	✓	✓	✓
OIG	✓	RNM	✓		✓	✓	✓	✓
RD	✓	✓	✓		✓	✓	99%	99%
RMA	✓	FR	✓		✓	✓	✓	✓

Figure 16: Sample USDA Scorecard

The USDA monthly scorecard is used to focus management attention on compliance to USDA policies and procedures, and to FISMA in the areas of Systems Inventory; C&A; POA&Ms; Contingency Planning; Scanning and Patching; Security Awareness, Privacy Basics and Specialized IT Training; Annual Assessments; Annual Security Plan Review; Privacy Impact Assessments; SORNs; FDCC Compliance Plan; Security Incidents; and Wireless scanning. (**NOTE**: Grey column indicates a requirement was not applicable for specific month(s).)

CSAM is the official repository for all FISMA artifacts. CSAM provides data for reports on POA&Ms, security controls and security categorization, which can be used to ensure further compliance with security policies and procedures as metrics, queries and reports are developed. In addition, reports are generated from the Cyber Security Incident Reporting Tracking Management (CSIRM) tool each week to identify status of incidents and help ensure they are being addressed in accordance with USDA policy and procedures.

4 Privacy and Other Oversight Activities

4.1 Privacy Initiatives

USDA worked on many privacy initiatives in FY 2008. In addition to enhancing the PII incident handling process, USDA reviewed all Privacy Impact Assessments (PIAs) and System of Record Notices (SORNs) to create an accurate baseline; assembled and formally chartered a Privacy Council with representatives from agencies and staff offices to address privacy-related requirements and issues; revised its PIA template; issued a social security number (SSN) policy plan for eliminating and/or ensuring its protection of PII and SSNs; and increased personnel awareness of Privacy.

4.1.1 Privacy Council

Figure 17: Privacy Council Meeting Title Slide

The Privacy Council has been officially assembled and chartered in FY 2008 to help address the protection of personal information and the requirements of federal privacy laws and regulations (e.g., Privacy Act of 1975 and E-Gov Act of 2002); OMB mandates such as Circular A-130, Appendix I; and other privacy-related directives. The Council provides a focused forum to review and recommend actions to the USDA Privacy Act Officer (PAO) and Senior Agency Official for Privacy (SAOP) on policy, procedures, practices, and programs that shape the protection of personal information maintained by the USDA; increase privacy security awareness of personnel at the USDA; and promote personnel responsibility in handling privacy information.

The Privacy Council meets monthly to discuss privacy issues, provide updates, form workgroups, and collaborate on improving the privacy program at the USDA. The Privacy Council is currently working on verifying the validity of SORNs not tied to IT systems; maintaining the integrity of the SORNs baseline; reviewing critical financial systems and systems with large boundaries to make sure information types are correct; attending CSAM training as needed; and taking as well as identifying personnel who need to be taking Privacy training covering Privacy laws, Privacy Threshold Analyses (PTAs), PIAs and SORNs.

4.1.2 SORN Completion Project

USDA has spent considerable effort in both FY 2007 and FY 2008 on obtaining an accurate SORN baseline. What began as a full review of 76 PIAs and 62 SORNs in FY 2007 continued in FY 2008 with the SORN completion project. The scope of the PIA/SORN projects was large since problems were eventually identified with 101 systems. These problems included:

- Privacy discrepancies/inconsistencies between privacy information in ASSERT©, PIA and/or SORN;
- PIA problems such as PIAs containing sensitive information, incomplete or vague information, the presence of personally identifiable information (PII), etc.; and
- No documentation on the SORN status.

PIAs have been corrected and resubmitted as a result of corrective action e-mails, concurrency reviews, and conversion of ASSERT© to CSAM in FY 2007 and FY 2008. Once the PIA baseline was stabilized, SORN completion e-mails were sent in FY 2008 to obtain and submit SORNs to the Office of the Secretary (OES).

During the first quarter of FY 2008, USDA agencies completed an inventory of systems containing PII. The inventory was adjusted from approximately 60 systems to over 90 systems containing PII. Privacy Council members are assuming the responsibility for verifying the SORN baseline each month, identifying any needed training, and making sure only up-to-date, relevant SORNs are posted.

4.1.3 Social Security Number Elimination and PII Reduction

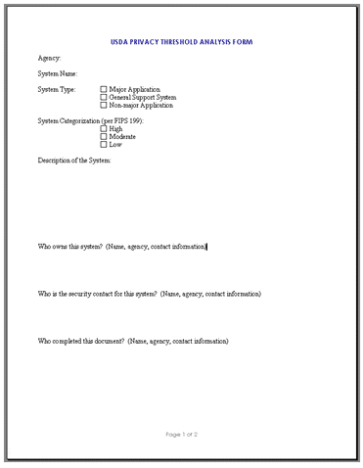
The Senior Agency Official for Privacy/Chief Information Officer issued a SSN Elimination Policy requiring agencies to submit plans for eliminating the use of SSNs in automated information systems unless required by statute. Agencies that were authorized by statute to use SSNs in their automated information systems were required to provide target dates or plans for encrypting the SSN information in their databases and masking SSNs on all system output both automated and manual. Agencies that could not eliminate SSN use in a timely manner are required to request an exception to the OCIO SSN Elimination policy. The Department has an overall deadline of September 30, 2008 to eliminate the use of unnecessary SSNs in information systems.

Much progress was made to reduce SSN usage. SSNs were removed or masked in the Department's Foundation Financial System, Travel Government Transportation Voucher System, T&A systems, and numerous personnel and payroll reports. Rural Development and Farm Service Agency also made substantial efforts to reduce usage of SSNs.

USDA is reviewing all web-based access to systems, servers and databases to ensure that all PII information is properly removed or masked; that no residual PII information remains on web server(s) that may still exist from prior uses of the server(s); and that all applications, which contained PII, have been reported to OCIO and entered into the CSAM inventory.

USDA has also modified its PIA form to ask if Privacy Act data contained in a system is "both relevant and necessary to the purpose for which the system is being designed." PIAs will be sampled to confirm that systems with PII actually require the information.

4.1.4 PTA and PIA



USDA PRIVACY THRESHOLD ANALYSIS FORM

Agency:

System Name:

System Type: ☐ Major Application ☐ General Support System ☐ Non-major Application

System Categorization (per FIPS 199): ☐ High ☐ Moderate ☐ Low

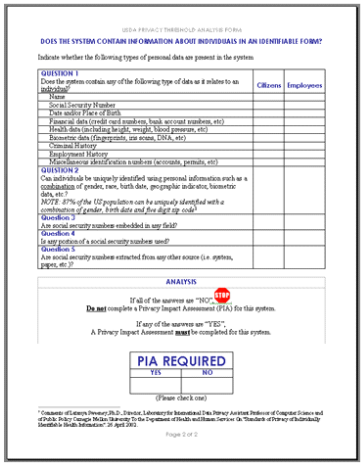
Description of the System:

Who owns this system? (Name, agency, contact information)

Who is the security contact for this system? (Name, agency, contact information)

Who completed this document? (Name, agency, contact information)

Page 1 of 2



USDA PRIVACY THRESHOLD ANALYSIS FORM

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to an individual?	Citizens	Employees
Name		
Social Security Number		
Date and/or Place of Birth		
Financial data (credit card numbers, bank account numbers, etc)		
Health data (including height, weight, blood pressure, etc)		
Biometric data (fingerprints, iris scans, DNA, etc)		
Criminal History		
Employment History		
Miscellaneous identification numbers (accounts, permits, etc)		
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc? *NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code*[1]		
Question 3 Are social security numbers embedded in any field?		
Question 4 Is any portion of a social security numbers used?		
Question 5 Are social security numbers extracted from any other source (i.e. system, paper, etc)?		

ANALYSIS

If all of the answers are "NO", STOP
Do not complete a Privacy Impact Assessment (PIA) for this system.

If any of the answers are "YES",
A Privacy Impact Assessment must be completed for this system.

PIA REQUIRED	
YES	NO

(Please check one)

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information" 26 April 2002

Page 2 of 2

Figure 18: Sample PTA Template

The PIA form was modified in FY 2008 to separate the initial analysis portion performed on every system from the rest of the PII assessment. The PTA form was created to be used in the initial analysis to determine whether a system contains PII. PTAs are required for every IT system, but only systems containing PII will require PIAs, and only systems containing PII that is retrieved by a unique personal identifier will require SORNs. PIAs have been created for all USDA IT systems containing PII.

4.1.5 Privacy and SORN Preparation Training

A training class for preparing Privacy Act-mandated SORNs was conducted in September 2008. This training was the first of several training sessions to be conducted onsite and/or via webinar with participants as determined by the Privacy Council. Topics being evaluated for possible inclusion in Privacy training sessions include privacy laws/legal framework, USDA overall privacy process, PTA/PIA/SORN preparation processes and procedures, rules of behavior, and consequences and corrective actions available for failure to follow USDA guidelines and/or Federal regulations.

4.1.6 Privacy Awareness Campaign

In addition to the privacy work discussed above, many awareness campaign activities related to privacy have been initiated and/or implemented in FY 2008, including flyers, banners, a video and a poster contest.

4.1.6.1 Privacy Awareness

Figure 19: Sample Awareness Day Poster Design

Privacy awareness activities in FY 2008 included posting a PII video on the intranet; updating the Privacy area of the intranet; distributing Awareness Day flyers to Information Systems Security Program Managers (ISSPMs) each month; and posting awareness flyers in buildings. Cyber Security is coordinating with the Office of Communications to print posters for transporting PII. These posters will be distributed to mailrooms and agencies Department-wide in a PDF file format for printing.

4.1.6.2 Privacy Logon Banner

Figure 20: Sample Privacy Logon Banner Designs

Over the last several months, USDA has piloted on-screen banners that appear after employees and contractors log into their workstations as part its PII awareness efforts. Currently, the banner is displayed on approximately 1400 employees' systems in the D.C. and Kansas City areas. The banner has had a positive effect in promoting PII awareness, and is being expanded Department-wide. It will be changed periodically to keep privacy concerns fresh in the minds of personnel as they log on. Cyber Security will be working with the Privacy Council, Awareness Committee and Telecommunications groups to develop alternative banners and make them more valuable to the USDA user community.

4.2 PRISMA

4.2.1 NISTIR 7358

The National Institute of Standards and Technology Interagency Report (NISTIR) 7358, *Program Review for Information Security Management Assistance (PRISMA)*, provides a database tool and reporting framework for conducting an independent review of the maturity of an agency's information security program. PRISMA incorporates standards from FIPS such as FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems*. It also incorporates guidelines from NIST Special Publications (SPs) such as NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*; existing federal directives including FISMA; and other proven techniques and recognized best practices in the area of information security.

4.2.2 PRISMA Description

PRISMA automates and consolidates the collection of data to satisfy USDA, NIST and OMB IT Security Program requirements; and provides a central data repository in a Microsoft Office format that is uniform, systematic and objective. PRISMA can be used to identify security program strengths and weaknesses; and provide a standard security program maturity assessment that can be measured against performance results of newly implemented processes. PRISMA can also facilitate the identification of agency or Department-wide security program weaknesses and vulnerabilities allowing IT managers to efficiently pinpoint resources and implement preventative security measures.

4.2.3 PRISMA Program at USDA

USDA conducted a PRISMA review on its certification and accreditation process; briefed the Information System Security Council (ISSC) community regarding the program; and held a special PRISMA meeting to provide a methodology overview and tool demonstration with guest speaker Pauline Bowen, co-author of NISTIR 7358. PRISMA implementation is currently not mandatory for USDA agencies, but is a suggested methodology, which may be mandated as the Department continues to standardize. PRISMA is being piloted this year. The pilot includes a review of three agencies. These three agencies have been selected based on their ability to provide a good baseline standard, their technical complexity, and the need to insure corrective measures and compliance due to recent incidents. The pilot also included volunteer agencies conducting self assessments and providing feedback on items such as labor, time, resources and practicality of the PRISMA tool. Information available in CSAM is leveraged for PRISMA reviews.

4.2.4 PRISMA Review – C&A and Information Security Planning

In addition to PRISMA reviews being conducted on three USDA agencies, a PRISMA review was conducted on the USDA for two topics: C&A and Information Security Planning. The results showed that the USDA has policies and procedures in place that are compliant with NIST requirements for all tested criteria in the C&A topic and for most tested criteria in the Information Security Planning (ISP) topic. The review also indicates substantial achievement on all higher levels of NIST-defined maturity for both topics. USDA is currently implementing recommendations based on findings to achieve full compliance with "Policy" and "Procedures" in both topic areas, laying the groundwork for reaching a fully "Implemented" maturity status.

4.3 Communication

4.3.1 Cyber Security Expo and Road Show

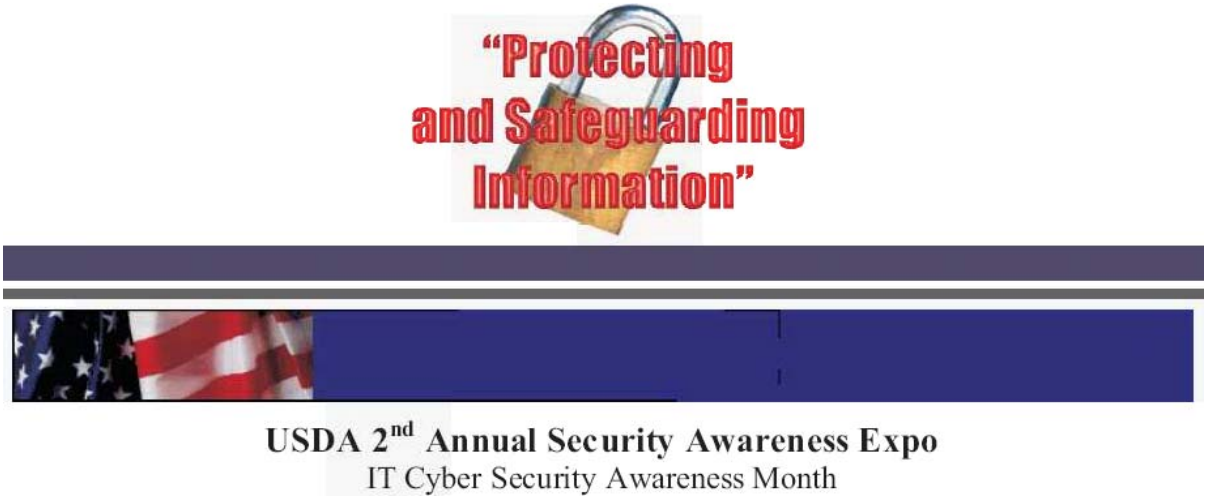


Figure 21: FY 2008 Security Awareness Expo Design

The Security Awareness theme in FY 2008 was on "Protecting & Safeguarding Information." The awareness tour began with a training "Road Show" in St. Louis on January 15, 2008. What started as the USDA Cyber Security Awareness Expo in FY 2007 with an intensive two-day exposition and series of presentations in Washington, D.C. went national in FY 2008. The tour included Fort Collins, Kansas City, Albuquerque and New Orleans, and concluded with an Expo in Washington, D.C.

The focus of the Expo and Road Show was on protecting the integrity of USDA program delivery by enhancing computer security and safeguarding PII. The training presented accomplished those goals for which attendees received specialized security training credits. The presentations included topics such as PII protection; disaster recovery planning and practices; incident handling; FDCC; the big picture on threats to information security; best practices for wireless security; and defense against identity theft.

4.3.2 Best Practices and Lessons Learned

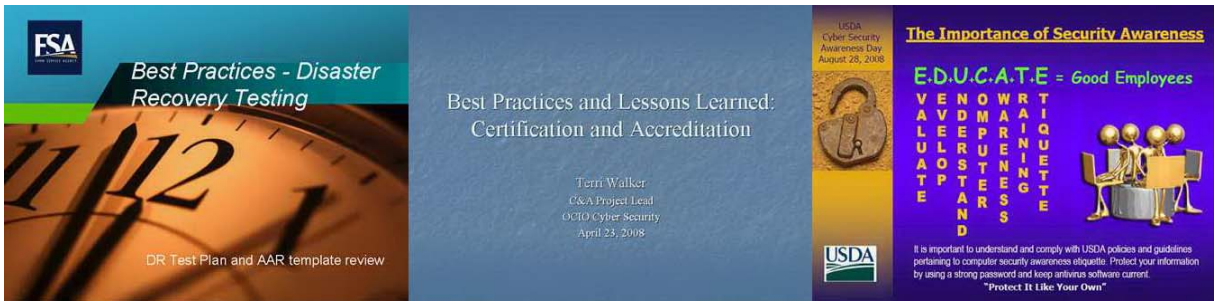


Figure 22: Sample Best Practices Slides

USDA provided monthly Best Practices and Lessons Learned presentations in FY 2008 on a number of topics including POA&Ms, FISMA, C&A, Incident Handling Reporting, and Disaster Recovery/Contingency Planning. USDA will continue to provide Best Practices and Lessons Learned on topics such as Privacy and Scanning Practices in FY 2008 and FY 2009. A list of Best Practices and Lessons Learned training scheduled with links to materials presented are available on the Cyber Security intranet area under Best Practices.

4.3.3 USDA Security and PII Awareness Campaign – Poster Contest

USDA kicked off a security and PII awareness campaign with a poster contest. This awareness campaign is designed to promote and market preventive measures in key areas of security, especially PII. USDA is asking every employee and contractor, working as a team, to help prevent security breaches, share information, and communicate measures to reduce PII incidents. The participation for the Poster Contest was excellent with over 100 entries received. The winning posters will be displayed at the third annual USDA Security Awareness Expo, on USDA PII awareness banners, and in other USDA activities and events to help promote awareness.

4.3.4 Cyber Security Awareness Day Flyers and Security Tips

Figure 23: Sample Awareness Day Poster Header

Awareness Day Flyers are distributed to ISSPMs each month to help promote awareness Department-wide. Posters are sent to agency employees, and posted in the front entrances, close to elevators, near the credit union and ATM machine, and in front of the cafeteria. Agencies are involved in this event to create a flyer on security to share Department-wide. The following awareness topics were addressed in FY 2008:

- Protecting and Safeguarding Information (10 Key Things Every Employee Should Remember);
- PII: Protect It Like Your Own (Identity Theft, Security Awareness);
- Report Suspicious Cyber Incidents;
- Avoiding Social Engineering and Phishing Attacks (Protect It Like Your Own Everyday);
- Network Password Standards;
- The Importance of Security Awareness – EDUCATE.

4.3.5 Security Tips

Three special security tips flyers were sent to ISSPMs in June 2008 to distribute and promote laptop security awareness. These flyers contained:

- Tips for Protecting Laptops from Thieves;
- Laptop Security Tips: How to Prevent a Loss or Theft; and
- Laptop Security Tips: How To Keep It from Getting Lost or Stolen.

4.3.6 OCFO/OCIO Connections Newsletter Articles

Several articles have been published in the Office of the Chief Financial Officer (OCFO) / OCIO *Connections* newsletter to promote understanding and awareness of security initiatives and activities such as Cyber Security Expo and Road Show, Computer Security Awareness and PII Training, EINSTEIN and FDCC. Article topics are selected to both inform and promote security practices within the USDA. Cyber Security will have a special spot in the newsletter to report and promote security and the PII awareness campaign for 2009.

4.4 Executive Steering Committee

The Executive Steering Committee (ESC) brings senior Department-level managers and agency managers together to rid the Department of its material IT weaknesses. The ESC addresses overarching IT issues, but also brings agencies to the table weekly to brief the committee on the status of correcting IT weaknesses. The ESC focuses on weaknesses identified by A-123 Appendix A, FISMA and other audits. The weekly agency briefings allow Department level managers to assist agencies, present best practices across the Department, and aid in addressing roadblocks.

4.4.1 Notable Achievements

The ESC's most notable achievements related to FISMA are: (1) holding agencies accountable for correcting weaknesses reported through the POA&M process; (2) working with agencies to ensure overarching IT issues are communicated to the ESC during agency weekly briefings, and; (3) influencing agencies to consistently use CSAM within the Department.

Other FISMA-related ESC achievements include making the decision to standardize on the NIST SP 800-53 control set for both FISMA and A-123 Appendix A initiatives, and choosing CSAM as the FISMA reporting tool based on its ability to integrate controls testing and serve as a central repository for all security and controls related issues. The ESC helped to focus agencies and stress the importance of efforts to ensure material weaknesses are adequately addressed, and to ensure internal controls are tested and documented at the level necessary for all reporting requirements.

4.4.2 Account Management

The ESC has decided to form an Account Management (AM) Working Group consisting of OCIO, OCFO and representatives from select USDA agencies to address issues related to removing access from users upon their separation from USDA and its respective agencies. Cyber Security has been assigned to manage the group. The AM Working Group has been tasked to develop:

- Consistent account management internal controls across USDA,
- A strategic plan for evolving account management into the final USDA Homeland Security Presidential Directive 12 (HSPD-12) solution,
- Full remediation and validation of current IT user account management internal control deficiencies within USDA, and
- Clear understanding of responsibilities between Service Providers and their customers in regards to account management.

The objectives for the AM Working Group are to:

- Plan effectively designed Departmental solutions and operational internal controls for Account Management within USDA.
- Identify clear responsibilities, actions and timelines for implementing, assessing and remediating internal controls regarding Account Management.
- Develop and communicate policies consistent with agreed-upon internal controls.
- Address any internal control interdependencies between Service Providers and their customers in regards to Account Management.

The AM Working Group drafted a project charter for a Departmental solution to manage account removals. Several issues have been raised such as the need for a policy to provide a process that can be managed by Service Providers and agencies; a solution that corresponds with long-term HSPD-12 solutions; a definition of account types; and realistic timeframes for maintaining account management. The group is also reviewing options for defining and maintaining reliable organizational structures to identify appropriate roles; leveraging AgLearn; facilitating access removals and replacements; focusing on controls as a hierarchy; and performing risk based analysis of separations. The team has been provided with a HSPD-12 update, and agrees that the AM approach must coincide with the HSPD-12 project effort.

4.5 Acquisition Approval Requests

The current USDA Acquisition Approval Request (AAR) process has incorporated standard security requirements from Federal Acquisition Regulation (FAR) 2007-004. AARs are reviewed to ensure cyber security considerations are included as applicable. AARs are part of the integrated governance process, and are required for every acquisition over $25,000. To assist with the process, USDA has created a new AAR website in FY 2008, which includes:

- An AAR Preparation and Submission Procedures area with an AAR Guidance draft document containing sections in checklist format.
- An USDA IT Policy and Standards area with links to policies, standards and memos applicable to the creation of AARs.
- A Blanket Purchase Agreements (BPAs) area containing links to BPAs recommended for acquiring servers, desktops, laptops and other IT equipment used Department-wide.

CS reviews IT-related AARs to ensure cyber security requirements are addressed and/or included in IT purchases. Cyber Security has performed over 140 reviews of AARs in FY 2008.

4.6 Information Security Sub-Council

Information Security Sub-Council (ISSC) members consist of agency ISSPMs, Cyber Security staff, and other security IT personnel. The ISSC communications in FY 2008 have been continuously improved to address security issues with best practices and other sessions held to supplement information disseminated in the regularly scheduled ISSC monthly meetings. The ISSC meetings in FY 2008 are used as a forum for ISSPMs and other security IT personnel to obtain updates, ask questions, receive answers, communicate, and collaborate on hot IT security issues impacting USDA Department-wide such as:

- AAR Process
- Antivirus and Scanning / Whole Disk Encryption / Safeboot / McAfee
- C&A / C&A Templates / Concurrency Reviews / POA&Ms / Interim Authorization to Operate (IATO) / Contractor Training and Systems / Scanning / Patching / Wireless
- CSAM (Conversion, Status, Training, A-123 Appendix A and FISMA Controls Incorporation and Testing, etc.)
- FDCC / Security Content Automation Protocol (SCAP)
- FISMA Requirements / Tools (i.e., ASSERT© / CSAM) / Security Program Reviews / PRISMA / Security Plans / Scorecards / Incident Detection, Response and Reporting
- HSPD-12 / Two Factor Authentication / LincPass / Non-Employee Information System (NEIS)
- Policies / Standard Operating Procedures / NIST Publications / Memos
- Privacy / SORN / PII / SSN Elimination Project / Privacy Act Data
- Testing (Penetration, Controls, Contingency Testing, etc.)
- Scorecards / President's Management Agenda (PMA) / Management Initiatives Tracking System (MITS)
- Training (CSAT, Privacy, Specialized Training, Cyber Security Awareness Month, Best Practices, etc.)
- Security Architecture Efforts / Enterprise Architecture Repository (EAR) / IT Governance
- ISSC Meeting Improvements / Information Risk Executive Council (IREC)
- Enterprise Contingency Planning Program (ECPP) / Living Disaster Recovery and Planning System (LDRPS) / Continuity of Operations (COOP) / IT Contingency Planning Work Group / Contingency Planning and Testing / Disaster Recovery

4.7 Security Information Management Readiness Assessment

The Security Information Management Readiness Assessment (SIMRA) is designed to determine an organization's readiness and anticipated effectiveness in designing and deploying a security information management (SIM) solution that addresses the SIM needs of the business. It examines how an organization can benefit from a SIM solution, and makes recommendations about people, process and technology changes needed to ensure alignment of electronic security practices with business goals and regulatory requirements based on the organization's feedback and information. The analysis is performed against industry best practices and recognized international standards such as ISO 17799. The objective in completing a SIMRA for USDA is to review areas of electronic security performance against business requirements and to report to management what areas appear to be effective and where changes should be made. Although USDA is not quite ready for a SIM solution, the SIMRA can help provide next steps to assist management in establishing a forward looking plan for information protection and risk management.

Appendix A. Acronyms

Acronyms used in this document are listed below in alphabetical order.

Acronym	Description
AAR	Acquisition Approval Request
AES	Advanced Encryption Standard
AM	Account Management
ASSERT©	Automated Security Self-Evaluation and Remediation Tracking
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CASF	Core Application Systems Framework
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
COOP	Continuity of Operations
CPWG	Contingency Planning Work Group
CS	Cyber Security
CSAC	Cyber Security Advisory Council
CSAM	Cyber Security Assessment and Management
CSAT	Computer Security Awareness Training
CSIRM	Cyber Security Incident Reporting Management
CSP	Comprehensive Security Program
CSSP	Cyber Security Service Program
DHS	Department of Homeland Security
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOD	Department of Defense
DoJ	Department of Justice
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
EAR	Enterprise Architecture Repository
ECCB	Enterprise Change Control Board
ECPP	Enterprise Contingency Planning Program
EDC	Enterprise Data Center
ESC	Executive Steering Committee

Acronym	Description
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Common Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTE	Full Time Employee
FTP	File Transfer Protocol
FY	Fiscal Year
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive
I-PARC	Inter-Agency Planning, Assessing and Remediating Controls
IATO	Interim Authorization to Operate
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPT	Integration Program Team
IRCG	Incident Response Core Group
IREC	Information Risk Executive Council
ISP	Information Security Planning
ISSC	Information Security Sub-Council
ISSLOB	Information Systems Security Line of Business
ISSPM	Information Systems Security Program Manager
IT	Information Technology
ITCP	IT Contingency Plan
ITS	Information Technology Services
LDRPS	Living Disaster Recovery and Planning System
MCATS	Master C&A Tracking Spreadsheet
MITS	Management Initiatives Tracking System
MOU	Memorandum of Understanding
NEIS	Non-Employee Information System
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget

Acronym	Description
P2P	Peer-to-Peer
PAO	Privacy Act Officer
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
PMA	President's Management Agenda
PMO	Project Management Office
POA&M	Plan of Action and Milestones
PRISMA	Program Review for Information Security Management Assistance
PTA	Privacy Threshold Analysis
SAIR	Situational Awareness and Incident Response
SAOP	Senior Agency Official for Privacy
SAR	Situational Awareness Report
SCA	Service Center Agencies
SCAP	Security Content Automation Protocol
SCD	Security Compliance Division
SIM	Security Information Management
SIMRA	Security Information Management Readiness Assessment
SOC	Security Operation Center
SOP	Standard Operating Procedure
SORN	System of Record Notice
SP	Special Publication
SSID	Service Set Identifier
SSN	Social Security Number
SSP	System Security Plan
TIC	Trusted Internet Connections
T2T	Tier 2 Training
US-CERT	United States Computer Emergency Readiness Team
USAID	United States Agency for International Development
USDA	United States Department of Agriculture (often referred as "Department")
UTN	Universal Telecommunications Network
VPN	Virtual Private Network
WAP	Wireless Access Point
WAR	Weekly Activity Report
WDE	Whole Disk Encryption

Appendix B. M-08-21 Required Attachments

B.1 Section B – CIO Report

The USDA M-08-21, Section B – Chief Information Officer Report is embedded below.

m08-21_section_b_ci
o_USDA08_FINAL_09

B.2 Section D – Senior Agency Official for Privacy

The USDA M-08-21, Section D – Senior Agency Official for Privacy Report is embedded below.

m08-21_section_d_s
aop_USDA08_FINAL_

Appendix C. Exhibits

Safeguarding
Against Responding

OCIO Sep 17th Call
for Implementation Pl

USDA_Incident_Notif
ication_Plan_FINAL[1