



United States Department of Agriculture

OFFICE OF INSPECTOR GENERAL





U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2014 Federal Information Security Management Act

Audit Report 50501-0006-12

What Were OIG's Objectives

Evaluate USDA's overall IT security program, compliance with FISMA, and effectiveness of controls over continuous monitoring, configuration management, identity and access management, incident response, assessments and authorizations, IT training, Plan of Action and Milestones, remote access management, contingency planning, contractor systems, and capital planning.

What OIG Reviewed

The scope was Departmentwide and included agency IT audit work completed during FY 2014, other OIG audits completed throughout the year, and the results of reviews performed by contract auditors. This audit covered 7 agencies and staff offices, operating 151 of the Department's 266 general support and major application systems in the systems inventory as of October 1, 2014.

What OIG Recommends

The Department should continue its progress by issuing critical policy and completing actions on the 34 outstanding recommendations from the FYs 2009 through 2013 FISMA audit reports and the 2 new recommendations included in this report.

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its IT security program and practices, during FY 2014.

What OIG Found

The Office of Inspector General (OIG) found that, although the Department of Agriculture (USDA) continues to improve the security posture of its information technology (IT) infrastructure and associated data, many longstanding weaknesses remain. In fiscal years (FY) 2009 through 2013, OIG made 55 recommendations for improving the overall security of USDA's systems, but the agreed upon corrective actions have been implemented for only 21. We noted that the Office of the Chief Information Officer (OCIO) is taking positive steps which should improve its security posture. For example, OCIO released five key Departmentwide policies in the latter part of FY 2013 and FY 2014. However, the next and most critical steps involve actions by each of USDA's agencies and staff offices. First, agency-specific procedures must be created based on each Departmental policy. Second, and most critical to improving USDA's security posture, each agency must incorporate the procedures it develops into its normal, ongoing business processes.

Again this year, we continue to report a material weakness in USDA's IT security. The Department has not (1) developed policies, procedures, or strategies for risk management in accordance with Federal guidance; (2) monitored agencies for compliance with baseline configurations and ensured known vulnerabilities were fixed; (3) deleted separated employees' access to computer systems; and (4) developed and implemented a policy to detect and remove unauthorized network connections.



United States Department of Agriculture
Office of Inspector General
Washington, D.C. 20250



November 7, 2014

The Honorable Shaun Donovan
Director
Office of Management and Budget
Eisenhower Executive Office Building
17th Street and Pennsylvania Avenue NW.
Washington, D.C. 20503

Dear Mr. Donovan:

Enclosed is a copy of our report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2014 Federal Information Security Management Act* (Audit Report 50501-0006-12), presenting the results of our audit of the Department of Agriculture's (USDA) efforts to improve the management and security of its information technology (IT) resources. USDA and its agencies have taken actions to improve the security over their IT resources; however, additional actions are still needed to establish an effective security program.

If you have any questions, please contact me at (202) 720-8001, or have a member of your staff contact Mr. Gil H. Harden, Assistant Inspector General for Audit, at (202) 720-6945.

Sincerely,

Phyllis K. Fong
Inspector General

Enclosure

Table of Contents

| | |
|---|-----------|
| U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2014 Federal Information Security Management Act | 1 |
| Findings and Recommendations..... | 1 |
| Recommendation 1 | 7 |
| Recommendation 2 | 7 |
| Background & Objectives | 8 |
| Scope and Methodology..... | 10 |
| Abbreviations | 11 |
| Exhibit A: Office of Management and Budget/Department of Homeland Security Reporting Requirements and U. S. Department of Agriculture Office of Inspector General Position | 12 |
| Exhibit B: Sampling Methodology and Projections | 43 |

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2014 Federal Information Security Management Act

Findings and Recommendations

This report constitutes the Office of Inspector General's (OIG) independent evaluation of the Department of Agriculture's (USDA) Information Technology (IT) security program and practices, as required by the Federal Information Security Management Act (FISMA) of 2002, and is based on the questions provided by the Office of Management and Budget (OMB)/Department of Homeland Security (DHS). These questions are designed to assess the status of the Department's security posture during fiscal year (FY) 2014. The OMB/DHS framework requires OIG to audit processes, policies, and procedures that had already been documented and implemented, and were being monitored during FY 2014.

The Office of the Chief Information Officer (OCIO) continues to take positive steps to improve the Department's security posture. OCIO released an additional five critical Departmentwide policies which, once implemented, will improve IT security within USDA. However, the next and most critical steps involve actions by each of USDA's agencies and staff offices. First, agency-specific procedures must be created based on each Departmental policy. Second, and most critical to improving USDA's security posture, each agency must incorporate the procedures it develops into its normal, ongoing business processes. OCIO needs to continue issuing policies but it also needs to prioritize one or two areas and begin a process to ensure agencies are creating and implementing procedures based on these policies. In order for USDA to attain a security posture that is secure and sustainable, all 34 of its agencies and offices must consistently implement Department policy based on a standard methodology. Once all of the Department's agencies and offices reach this level of compliance with security policies, USDA's security posture will be consistent, effective, and sustainable. The degree to which USDA, as a whole, complies with FISMA and other security guidance is based on the security posture of each of its agencies and offices. If each agency is in compliance with the Department's policies, then USDA as a whole will be FISMA compliant and, more importantly, more secure.

USDA is working to improve its IT security posture, but many longstanding weaknesses remain. We continue to find that OCIO has not implemented corrective actions that the Department has committed to in response to prior OIG recommendations. In FYs 2009 through 2013, OIG made 55 recommendations for improving the overall security of USDA's systems, but only 21 of these have been closed (i.e., the agreed upon corrective action has been implemented). Our testing identified that security weaknesses still exist in 3 of the 21 closed recommendations. Because of these identified outstanding recommendations and weaknesses, we continue to report a material weakness in USDA's IT security that should be included in the Department's Federal Managers Financial Integrity Act report.

USDA is a large, complex organization that includes 34 separate agencies and staff offices, most with their own IT infrastructure. Each of USDA's 34 agencies and staff offices, including OCIO, need to be held accountable for implementing the Department's policies and procedures.

Once compliance by all agencies is attained, then FISMA testing results should be similar, regardless of which agency is selected and tested, and the Department's overall security posture should improve.

The following summarizes the key matters discussed in Exhibit A of this report, which contains OIG's responses to the OMB/DHS questions. These questions were defined on the DHS CyberScope FISMA reporting website.

To address the FISMA metrics, OIG reviewed IT systems and agencies,¹ OIG independent contractor audits, annual agency self-assessments, and various OIG audits throughout the year.² Since the scope of each review and audit differed, we could not use every review or audit to address each question.

During our review we found that USDA has established a continuous monitoring program. Specifically, we found that the Department has issued a policy, as well as procedures, for continuous monitoring. The Department provided a draft strategy for developing an enterprise-wide continuous monitoring plan; however, it has not been issued. We also found 5 of 33 systems where ongoing assessments of selected security controls had not been performed in FY 2014. In the FY 2010 FISMA report, we recommended that the Department ensure system authorizing officials and other key system officials be provided with security status reports covering updates to system security plans (SSP) and security assessment reports (SAR), as well as additional Plan of Action and Milestones (POA&M). OCIO agreed and estimated that this would be implemented by September 30, 2011; however, the recommendation remains open.

The Department has established, and is maintaining, a security configuration management program; however, there are opportunities for improvement. Specifically, we found that the Department has established adequate policy, and has made standard baseline configurations available for all applicable operating systems; however, agencies have not followed the policy or baselines when configuring servers and workstations. At one agency we found over 59 percent of the National Institute of Standards and Technology (NIST) baseline settings for production servers had deviations without the proper documentation. In the FY 2010 FISMA audit, OIG recommended the Department ensure scanning be performed to assess compliance to the baseline configurations and to identify vulnerabilities, as required by NIST. This recommendation remains open; OCIO has exceeded its estimated implementation date of August 30, 2011.

The Department has established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines to identify users and network devices. For example, the Department has developed an account and identity management policy that is compliant with NIST standards and has adequately planned for

¹ Two of the agencies selected received IT support from a third USDA agency; we did test that agency, where applicable, and included the results in our sampled agencies' questions.

² Agency annual self-assessments derive from OMB Circular A-123, which defines *Management's Responsibilities for Internal Control in Federal Agencies* (December 21, 2004). The circular requires agency management to annually provide assurances on internal control in Performance and Accountability Reports. During annual assessments, agencies take measures to develop, implement, assess, and report on internal controls, and take action on needed improvements.

Personal Identification Verification (PIV) implementation for logical and physical access, in accordance with Government standards.³ Additionally, agencies were able to identify devices, users, and non-users who access the organization's systems and networks. The Department is also moving towards a centralized enterprise solution for access management which should provide a standardized system that automates network management. However, our testing identified opportunities for improvement. We found that agencies did not ensure that users were granted access based on need and agencies did not terminate or deactivate employee accounts when access was no longer required. For example, we found nine separated users in one agency that still had active accounts. Departmental policy requires that accounts be disabled within 48 hours of an employee's separation.⁴

The Department has established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, the newly issued incident policy did not include the required NIST element of performance measures.⁵ Although USDA's incident handling has improved, we continue to find that the Department is not consistently following its own policy and procedures in regard to incident response and reporting (i.e., we identified four incidents that were the result of a lost or stolen device and were not promptly reported to OCIO by the agency). Based on our sample results, we estimate that 300 (18 percent) of 1,670 incidents were not handled in accordance with Departmental procedures.^{6,7} Additionally, of the 300 not handled in accordance with procedures, we estimate that USDA did not report 171 incidents (10 percent) to the United States-Computer Emergency Response Team (US-CERT) within the required timeframe.⁸

We determined USDA has procured the tools to correlate incidents across the Department but has not deployed them effectively. As a result, USDA does not have the ability to correlate incidents across its entire network infrastructure. Based on tests of USDA's cloud traffic, discussions with USDA IT personnel, and our review of the cloud provider's service agreement and incident plan, we also determined that the Department is not capable of managing risks in this virtual/cloud environment. USDA lacks the ability to track cloud traffic, the cloud service provider does not have its own Data Loss Prevention (DLP) solution deployed, and the service

³ The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12* (HSPD-12), originally issued in August 2004, requires Federal agencies to develop and deploy for all of their employees and contract personnel a PIV credential which is used as a standardized, interoperable card capable of being used as employee identification and allows for both physical and information technology system access.

⁴ DR 3505-003, *Access Control Policy* (August 11, 2009).

⁵ NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (August 2012).

⁶ Agriculture Security Operations Center (ASOC) Computer Incident Response Team, Standard Operating Procedure SOP-ASOC-001, Standard Operating Procedures for Reporting Security and Personally Identifiable Information Incidents (June 9, 2009).

⁷ We are 95 percent confident that between 158 (9 percent) and 442 (26 percent) incidents were not handled in accordance with Departmental procedures. Additional sample design information is presented in Exhibit B.

⁸ US-CERT provides response support and defense against cyber-attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. NCSD was established by DHS to serve as the Federal Government's focal point for cyber security coordination and preparedness.

agreement between USDA and its cloud service provider does not include the appropriate provisions outlining each party's incident reporting roles and responsibilities.⁹

We found that the Department has not established a Risk Management Framework (RMF) program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.¹⁰ The Department has issued a guide that addresses parts of the six-step RMF process and is in the beginning phases of planning for an overall RMF program. Although improvements have been made, we continue to find inadequate documentation. Also, in order for a system to become operational, NIST SP 800-37 requires USDA agencies to follow the RMF process to obtain an authorization to operate (ATO) and to effectively manage risk for their systems. In order for an ATO to be granted, systems must be categorized, controls identified and implemented, risks assessed, and the final concurrency review examined to proceed with accreditation. We found five systems that were operational without an ATO. The Department said these systems were necessary for USDA operations and therefore needed to operate without an ATO for business reasons. Also, the Department has 50 systems with expired ATOs, including the Cyber Security Assessment and Management (CSAM) system, the Department's repository for all FISMA systems.¹¹ In the FY 2012 FISMA report, OIG recommended the Department verify that all systems have the proper ATO prior to implementation. Management decision has been reached, but OCIO has exceeded the estimated completion date of September 30, 2013. As a result, these systems are operational, but without proper security certification, which leaves the agencies and the Department vulnerable because the systems have not been through proper security testing.

The Department has established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The Department and the two agencies we tested had policy¹² and procedures that met all NIST requirements for annual security awareness training and specialized security training.¹³ Additionally, the Department

⁹ DLP is the ability "to detect inappropriate transport of sensitive information. Examples of sensitive content are personal identifiers (e.g. credit card or Social Security numbers) or corporate intellectual property."

¹⁰ RMF is a NIST publication. The publication promulgates a common framework which is intended to improve information security, strengthen risk management, and encourage reciprocity between Federal agencies. NIST Special Publication (SP) 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), was developed by the Joint Task Force Transformation Initiative Working Group. OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

¹¹ CSAM is a comprehensive system developed by the Department of Justice, which can facilitate achieving FISMA compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staffs to (1) manage their system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as SSPs, SARs, and internal security control assessments; and (4) generate custom and pre-defined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems as well as those operated by contractors on the agency's behalf.

¹² DR 3545-001, Information Security Awareness and Training Policy (October 22, 2013).

¹³ Departmental SOP-Cyber and Privacy Policy and Oversight-018, *Information Security Awareness Training* (April 21, 2011).

provided role-based security training to personnel with assigned security roles and responsibilities.¹⁴

The Department has established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines which tracks and monitors known information security weaknesses.¹⁵ However, our testing identified some areas for improvement. For example, agencies were not creating POA&Ms for unresolved vulnerabilities existing for over 30 days, as required by Departmental policy.¹⁶ In addition, our review of POA&Ms within CSAM found that agencies were not adequately detailing plans for remediation and were not including proper supporting documentation for effective closure. We estimate that 213 of the 853 POA&Ms that were closed during FY 2014 had remediation actions that did not sufficiently address the identified weakness.¹⁷ We also noted that priority levels are not being identified in CSAM for each POA&M and that milestone dates were not always adhered to.

The Department has established a remote access program that is consistent with FISMA requirements and OMB policy. However, our testing identified that Departmental policies for remote access and teleworking did not meet NIST requirements.¹⁸ Specifically, we found one agency did not have a fully developed remote access policy or associated procedures. This occurred because the agency used a remote access service provider who did not provide policy and procedures. In our FY 2010 FISMA report, we recommended that the Department update its policy and procedures to be NIST-compliant. This recommendation is still open and OCIO has exceeded its estimated completion date of August 31, 2011. We also found that while the Department and agencies were monitoring, detecting, and reporting unauthorized (rogue) network connections, there are no documented policies that require it. This occurred because the draft Departmental policy had not been issued. USDA requires multi-factor authentication (i.e., two means of identification) for all remote access and both agencies we reviewed had implemented it.¹⁹

¹⁴ NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations* (April 2013).

¹⁵ A POA&M is a tool that identifies tasks needing to be accomplished to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of efforts to correct security weaknesses found in programs and systems. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and scheduled completion dates for the milestones. The goal of a POA&M should be to reduce the risk of the weakness identified.

¹⁶ Departmental Manual (DM) 3530-001 requires a POA&M to be developed in accordance with FISMA reporting requirements for any unresolved critical vulnerabilities existing for more than 30 days from the date of the scan.

¹⁷ We are 95 percent confident that between 113 (13 percent) and 314 (37 percent) of closed POA&Ms in the fiscal year had remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies. Additional sample design information is presented in Exhibit B.

¹⁸ DM 3525-003, *Telework & Remote Access Security* (February 17, 2005) and NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009).

¹⁹ Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the Department of Defense (DoD) common access card. DR 3505-003, *Access Control Policy* (August 11, 2009).

The Department has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, our testing identified opportunities for improvement. Specifically, Departmentwide, we found that 100 of 266 systems did not have evidence of annual testing of contingency/disaster plans, as required by NIST and the Department.²⁰ Also, based on our sample results, we estimate that 136 systems (61 percent) did not have evidence of ongoing testing.²¹ We found the template provided to agencies for contingency planning purposes was updated, available to the agencies, and contained all of the NIST-required elements. In addition, during our detailed testing at two agencies, we found that all 32 of their plans were developed with the appropriate information required by NIST.

We found that the Department has now established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in a cloud environment external to the organization. However, the Department's policy was not issued until August 12, 2014. In addition, FISMA requires USDA to maintain a complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud. We identified 31 USDA cloud systems and found 23 were not listed in the inventory. We reviewed 19 operational contractor systems in USDA's inventory and found 16 systems with no or unsigned SSPs, 6 systems with an expired ATO, and 3 systems with insufficient interconnection documentation.

Our testing of USDA's capital planning process determined the Department has established and maintains a capital planning and investment program for information security. However, we continue to find that OCIO has not implemented corrective actions to resolve recommendations that the Department had committed to as part of the management decision process. In the FY 2012 FISMA audit, we recommended that USDA incorporate a review of line items in the annual Capital Planning cycle to verify that information security resources requested by the agencies were accompanied by the required supporting documentation. Our testing found the weakness related to unsupported agency Exhibit 53 documentation continued to exist.²² The agencies stated that they were unaware of the need to retain adequate supporting documentation used for the budgeting process at the time of the budget submission. One agency, however, has since started to maintain supporting documentation for its current security capital planning and investment program budget requests.

The following recommendations are new for FY 2014. Because 34 recommendations from FYs 2009 through 2013 have not been closed, we have not made any repeat recommendations. If the plans initiated to close out the FY 2009 through 2013 recommendations are no longer achievable, due to budget cuts or other reasons, then OCIO needs to update those closure plans and request a change in management decision, in accordance with Departmental guidance.

²⁰ *USDA Contingency Plan Exercise Handbook, Rev. 1.1* (February 2011).

²¹ We are 95 percent confident that between 108 (49 percent) and 164 (74 percent) systems did not have evidence of ongoing testing. Additional sample design information is presented in Exhibit B.

²² Exhibit 53 is a required OMB submitted package that includes the Agency IT Investment Portfolio, providing budget estimates for overall IT investments and for major and significant IT systems.

Recommendation 1

Finalize and implement the strategy for developing an enterprise-wide continuous monitoring plan.

Recommendation 2

Update the Department's Incident Policy to include performance measures.

Background & Objectives

Background

Improving the overall management and security of IT resources needs to be a top priority for USDA. Technology enhances users' abilities to share information instantaneously among computers and networks, but it also makes organizations' information residing on networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources. Insiders with malicious intent, recreational and institutional hackers, and attacks by foreign intelligence organizations are a few examples of threats to the Department's critical systems and data.

On December 17, 2002, the President signed into law the e-Government Act (Public Law 107-347), which includes Title III, FISMA. FISMA permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. FISMA continued the annual review and reporting requirements introduced in GISRA, and also included new provisions that further strengthened the Federal Government's data and information systems security, such as requiring the development of minimum control standards for agencies' systems. NIST was tasked to work with agencies in developing standards as part of its statutory role in providing technical guidance to Federal agencies.

FISMA also supplements the information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996. The Act is consistent with existing information security guidance issued by OMB and NIST. More importantly, however, FISMA consolidated these separate requirements and guidance into an overall framework for managing information security. It established new annual reviews, independent evaluations, and reporting requirements to ensure agency compliance. It also provided for both OMB and Congressional oversight.

FISMA assigned specific responsibilities to OMB, agency heads, Chief Information Officers (CIO), and Inspectors General. OMB is responsible for establishing and overseeing policies, standards, and guidelines for information security. The responsibilities include the authority to approve agencies' information security programs. OMB also requires the submittal of an annual report to Congress summarizing the results of agencies' evaluations of their information security programs. Instructions for FY 2014 FISMA reviews are outlined in OMB Memorandum (M)-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*. DHS uses the CyberScope website to consolidate the reporting.

Each agency must establish a risk-based information security program that ensures information security is practiced throughout the lifecycle of each agency's system. Specifically, the agency's CIO must oversee this program which, following OMB M-07-24 must include:

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems and data supporting critical operations and assets;

- development and implementation of risk-based, cost-effective policies and procedures to provide security protections for the agency's information;
- training that covers security responsibilities for information security personnel and security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of security policies, procedures, controls, and techniques;
- processes for identifying and remediating significant security deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- annual program reviews by agency officials.

In addition, FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and a compliance assessment. The evaluations are to be performed by the agency's Inspector General or an independent evaluator, and the results of these evaluations are to be reported to OMB.

Objectives

The objective of this audit was to evaluate the status of USDA's overall IT security program by evaluating the:

- effectiveness of the Department's oversight of agencies' IT security programs, and compliance with FISMA;
- agencies' systems of internal controls over IT assets;
- the Department's progress in establishing a Departmentwide security program, which includes effective assessments and authorizations; and
- agencies' and the Department's POA&M consolidation and reporting process; and the effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, contractor systems, and IT capital planning.

Scope and Methodology

The scope of our review was Departmentwide and included agency IT audit work completed during FY 2014. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Fieldwork for this audit was performed from March 2014 through October 2014. In addition, this report incorporates audits done throughout the year by OIG. Testing was conducted at offices in the Washington, D.C. and Kansas City, Missouri, areas. Additionally, we included the results of IT control testing and compliance with laws and regulations performed by contract auditors at four additional USDA agencies. In total, our FY 2014 FISMA audit work covered seven agencies and staff offices:

- Food and Nutrition Service,
- Farm Service Agency,
- Natural Resources Conservation Service,
- Office of the Chief Financial Officer,
- OCIO,
- Risk Management Agency, and
- Rural Development.

These agencies and staff offices operate 151 of the Department's 266 general support and major application systems.

To accomplish our audit objectives, we performed the following procedures:

- Consolidated the results and issues from our prior IT security audit work and the work contractors performed on our behalf. Contractor audit work consisted primarily of audit procedures found in the U.S. Government Accountability Office's (GAO) *Financial Information System Control Audit Manual*.
- Performed detailed testing specific to FISMA requirements at selected agencies, as detailed in this report.
- Gathered the necessary information to address the specific reporting requirements outlined in OMB M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*. DHS uses the website CyberScope to consolidate the reporting.
- Evaluated the Department's progress in implementing recommendations to correct material weaknesses identified in prior OIG and GAO audit reports.
- Performed statistical sampling for testing where appropriate. Additional sample analysis information is presented in Exhibit B.

We compared test results against NIST controls, OMB/DHS guidance, e-Government Act requirements, and Departmental policies and procedures for compliance.

Abbreviations

| | |
|--------------|---|
| A&A..... | Assessment and Authorization |
| ASOC..... | Agriculture Security Operations Center |
| ATO..... | Authorization to Operate |
| BIA..... | Business Impact Analysis |
| CIO..... | Chief Information Officer |
| CISO..... | Chief Information Security Officer |
| CSAM..... | Cyber Security Assessment and Management |
| DHS..... | Department of Homeland Security |
| DLP..... | Data Loss Prevention |
| DM..... | Departmental Manual |
| DoD..... | Department of Defense |
| DR..... | Departmental Regulation |
| FedRAMP..... | Federal Risk and Authorization Management Program |
| FISMA..... | Federal Information Security Management Act |
| FY..... | Fiscal Year |
| GAO..... | Government Accountability Office |
| GISRA..... | Government Information Security Reform Act |
| HSPD-12..... | Homeland Security Presidential Directive-12 |
| IP..... | Internet Protocol |
| ISA..... | Interconnection Security Agreement |
| ISCM..... | Information Security Continuous Monitoring |
| IT..... | Information Technology |
| MOU..... | Memorandum of Understanding |
| NCSD..... | National Cyber Security Division |
| NIST..... | National Institute of Standards and Technology |
| OCIO..... | Office of the Chief Information Officer |
| OIG..... | Office of Inspector General |
| OMB..... | Office of Management and Budget |
| OS..... | Operating System |
| PIV..... | Personal Identification Verification |
| POA&M..... | Plan of Action and Milestones |
| RMF..... | Risk Management Framework |
| SAP..... | Security Assessment Plan |
| SAR..... | Security Assessment Report |
| SOP..... | Standard Operating Procedure |
| SP..... | Special Publication |
| SSP..... | System Security Plan |
| USGCB..... | United States Government Configuration Baseline |
| US-CERT..... | US-Computer Emergency Response Team |
| USDA..... | Department of Agriculture |

Exhibit A: Office of Management and Budget/Department of Homeland Security Reporting Requirements and U. S. Department of Agriculture Office of Inspector General Position

OMB/DHS' questions are set apart using boldface type in each section. We answered direct questions with either boldface Yes or No.

The universe of systems and agencies reviewed varied during each audit or review included in this report. As part of FISMA, OIG reviewed: systems and agencies, audit work conducted for OIG by independent public accounting firm contractors, annual agency self-assessments, and various OIG audits conducted throughout the year.²³ Since the scope of each review and audit differed, we could not use every review or audit to answer each question.

The audit team reviewed all 11 FISMA areas and we incorporated statistical sampling into 3 review areas. Each of the three areas was represented by the relevant universe associated with it. The specific sample designs are summarized in Exhibit B.

S1: Continuous Monitoring Management

1.1 Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

1.1.1 Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). – Yes

No exception noted. The Department has developed the RMF guidance and has published the DR policy entitled Security Assessment and Authorization in regards to continuous monitoring. Additionally, we identified two of two agencies reviewed that had an agency procedure in place for continuous monitoring.²⁴

1.1.2 Documented strategy for information security continuous monitoring (ISCM). – No

The Department provided a strategy for developing an enterprise-wide continuous monitoring plan. However, this strategy was in draft and has not been implemented. OCIO also provided

²³ Agency annual self-assessments are required by OMB Circular A-123, *Management's Responsibility for Internal Control* (December 21, 2004), which defines management's responsibility for internal controls in Federal agencies. The Circular requires agencies' management to annually provide assurances on internal control in its Performance and Accountability Report. During the annual assessment, agencies take measures to develop, implement, assess, and report on internal control, and to take action on needed improvements.

²⁴ NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations* (April 2013). CA-7 requires the organization to establish a continuous monitoring strategy and program.

OIG with the USDA Information Security Continuous Monitoring (ISCM) Program Charter.²⁵ This document contains objectives and milestones that OCIO believes are necessary to improve continuous monitoring within agencies and the Department. Additionally, the Department has a variety of continuous monitoring tools that have benefited its security posture. For example, the Department has a network tool that, although not fully operational, was being used to actively monitor for malicious activity within the USDA network.²⁶ Furthermore, USDA has been actively using another tool to help standardize and centralize the governance of its workstations and servers.

In the FY 2010 FISMA report, we recommended that the Department develop policies, procedures, strategies, and implementation plans for continuous monitoring, including items such as vulnerability scanning, log monitoring, notification of unauthorized devices, and sensitive new accounts in accordance with NIST. Although the Department has implemented policies and procedures for continuous monitoring, it still lacks a finalized strategic plan. The Department reported final action on the recommendation on September 30, 2011; however, OIG found the condition to still be present.

1.1.3 Implemented ISCM for information technology assets. – No

The Department provided an ISCM strategic plan for developing an enterprise-wide continuous monitoring plan. However, this strategy was in draft and has not been implemented.

1.1.4 Evaluate risk assessments used to develop their ISCM strategy. – No

No documented risk assessment was provided. The Department provided an ISCM strategic plan for developing an enterprise-wide continuous monitoring plan. However, this strategy was in draft and has not been implemented.

1.1.5 Conduct and report on ISCM results in accordance with their ISCM strategy. – No

The Department provided an ISCM strategic plan for developing an enterprise-wide continuous monitoring plan. However, this strategy was in draft and has not been implemented.

1.1.6 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A). – No

We identified 5 of 33 systems where ongoing assessments of selected security controls had not been performed in FY 2014.²⁷ The agencies that own these systems have no assurance that their

²⁵ Program Charter, *U.S. Department of Agriculture Strategic Plan for Information Security Continuous Monitoring (ISCM)* (February 2014).

²⁶ When a sensor is not inline, traffic does not flow through the sensor. The sensor instead analyzes a copy of the monitored traffic. The advantage of operating this way is that the sensor does not affect network performance. The disadvantage of operating in this mode, however, is that the sensor cannot actively stop malicious traffic from reaching its intended target. The response actions implemented by the sensor devices are post-event responses.

²⁷ The 33 major applications were reported in CSAM as of October 1, 2014.

controls will remain effective over time, as changes occur in threats, missions, operational environments, and technologies.

1.1.7 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). – Yes

No exception noted. We found that all agencies reviewed were able to verify that the required information was provided to the authorizing official or other key system officials.

In the FY 2010 FISMA report, we recommended that the Department ensure system authorizing officials and other key system officials be provided with security status reports covering updates to SSPs and SARs, as well as additional POA&Ms. The recommendation remains open and exceeded the estimated completion date of September 30, 2011.

1.2 Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was not noted in the questions above.

No additional information was provided.

S2: Configuration Management

2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

2.1.1 Documented policies and procedures for configuration management. – Yes

No exception noted. NIST requires that the organization develop formal documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.²⁸ OIG found the configuration management program includes adequate documented policies and procedures at both the Department and agency level.

2.1.2 Defined standard baseline configurations. – No

NIST requires the organization to develop, document, and maintain as part of its configuration control, a current baseline configuration of the information system.²⁹ The Department has issued

²⁸ NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (August 2013). Control CM-1 requires that a formal documented configuration management policy and procedures be developed.

²⁹ NIST SP 800-70 Rev. 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers Recommendations* (February 2011).

policy stating USDA agencies and staff offices shall apply secure baseline configurations for all hardware and software products using the NIST guidelines.³⁰ OIG found that the configuration management program includes defined standard baseline configurations and agencies are required to use baselines on all systems; however, two agencies self-reported a problem with standard baseline configurations.

2.1.3 Assessments of compliance with baseline configurations. – No

NIST requires the organization to develop, document, and maintain a current baseline configuration of each information system. We found over 59 percent of the settings on the Windows servers at one agency were not compliant with the baseline configurations nor were the deviations sufficiently documented. In addition, two other agencies self-reported a deficiency with baseline configurations and the contractor reviews also identified one agency with a baseline configuration deficiency.

In the FY 2009 FISMA report, we recommended that the Department implement effective policies and procedures to ensure agencies use required NIST and Departmental configuration checklists and document the reasons for those settings not implemented. OCIO has exceeded its estimated completion date of July 30, 2011.

Also, in the FY 2010 FISMA report, we recommended that the Department ensure documented configuration management procedures are developed and consistently implemented across the Department, including baseline configurations for all approved software and hardware. Any changes to the baseline guides should be documented and approved. OCIO has exceeded its estimated completion date of September 30, 2011.

2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result deviations. – No

We found that two agencies reviewed did not have a process for timely remediation of scan result deviations. Specifically, OIG reviewed scan results from the agencies and found one with over 37 percent of the vulnerabilities that were not mitigated within six months and a second with over 13 percent that were not mitigated in five months.³¹ Additionally, four agencies self-reported that they had an issue with the process for timely remediation of scan result deviations, as specified in organization policy or standards. As a result, networks and devices within the Department are at risk of compromise.

³⁰ DR 3520-002, *Configuration Management* (August 12, 2014).

³¹ A vulnerability scan is the process of determining the presence of known vulnerabilities by evaluating the target system over the network. DM 3530-001, *USDA Vulnerability Scan Procedures* (July 20, 2005), requires that vulnerability scans are to be performed on a monthly basis for all existing and new networks, systems, servers, and desktops by duly authorized users in accordance with established procedures.

2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. – No

NIST requires the organization to establish and document mandatory security configuration settings for information technology products utilized within the information system. One such requirement is the United States Government Configuration Baseline (USGCB) secure configurations for user workstations and laptops.³² We found that the Department has a 90 percent USGCB compliance rate. However, although 18 USDA entities had deviations, we found only 6 had the required documented waivers for those deviations.³³ In addition, contractor reviews identified an agency with deviations from the USGCB settings. These missing standards make the laptops and workstations less secure and users and user information more susceptible to compromise.

In the FY 2013 FISMA report, OIG recommended the Department monitor agencies' workstations for USGCB compliance. The recommendation is still open, and OCIO has exceeded its estimated completion date of September 30, 2014.

2.1.6 Documented proposed or actual changes to hardware and software configurations. – Yes

No exception noted. NIST requires the organization to document approved configuration-controlled changes to the system. OIG did not identify any problems with the documentation for proposed or actual changes to hardware and software configurations of the agencies reviewed.

2.1.7 Process for timely and secure installation of software patches. – No

NIST requires the organization to identify and correct system flaws and incorporate flaw remediation (known as vendor patches) into the organizational configuration management process.³⁴ We found both agencies reviewed had not implemented a process for timely and secure installation of software patches. Specifically, at one agency, OIG found 24,301 of 29,459 (82.5 percent) vulnerabilities were not corrected with an available patch from the vendor. As a result, systems are at risk of compromise when they could have been secured had the available patch been applied.

In the FY 2010 FISMA report, OIG recommended that the Department develop automated procedures for the timely and secure installation of software patches. The recommendation is still open, and OCIO has exceeded its estimated completion date of June 15, 2011.

³² OMB M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems* (March 22, 2007), requires agencies to adopt the security configurations developed by NIST, the Department of Defense, and DHS.

³³ DR 3520-002, *Configuration Management* (August 12, 2014), requires agencies to submit a request for waiver annually for any deviation from the USGCB baseline.

³⁴ A patch is a small piece of software that is used to correct a problem with a software program or an operating system. Most major software companies will periodically release patches, usually downloadable from the internet, that correct very specific problems or security flaws in their software programs.

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). – No

The Department requires all agencies to establish and implement procedures for accomplishing vulnerability scanning of all networks, systems, servers, and desktops for which they have responsibility. This includes performing monthly scans and remediating vulnerabilities found as a result of the scans. We found two of two agencies reviewed had not implemented software assessing (scanning) capability. Specifically, we found that agencies were not mitigating vulnerabilities or creating POA&Ms as required by NIST. Additionally, four agencies self-reported and one contractor review identified a problem with timely remediation of scan results.

In the FY 2010 FISMA report, OIG recommended that the Department ensure scanning is performed as required by NIST for compliance with the baseline configurations and for vulnerabilities. This recommendation is open and has exceeded the estimated completion date of August 30, 2011.

In addition, OIG recommended in the FY 2011 FISMA report that the Department develop monitoring procedures to verify that monthly vulnerability scans are completed as required by Departmental guidance. This recommendation is open and has exceeded the estimated completion date of July 30, 2013.

2.1.9 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2) – No

NIST requires Federal agencies to establish and document mandatory configuration settings for information technology products employed within the information system, and to implement the recommended configuration settings. OIG found that two of two agencies reviewed did not remediate configuration vulnerabilities. Specifically, we found 227 configuration-related vulnerabilities on 13 websites maintained by the agencies that were not remediated.³⁵ Consequently, the websites are at risk for compromise. Additionally, agency self-inspections identified four of six agencies that do not remediate configuration vulnerabilities in a timely manner.

2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2). – No

NIST requires Federal agencies to incorporate vendor software flaw remediation (patches) into the organizational configuration management process. We found both agencies reviewed had not implemented a process for timely and secure installation of software patches. Specifically, at one agency OIG found 24,301 of 29,459 (82.5 percent) vulnerabilities were not corrected with an available patch from the vendor. As a result, systems are at risk of compromise when they could have been secured, had the available patch been applied.

³⁵ We utilized a commercially available software package designed to thoroughly analyze web applications and web services (websites) for security vulnerabilities.

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

OIG reviewed computers in use at USDA specifically looking for operating systems (OS) in use past their end-of-life. We found 77 machines at 8 agencies that were using OS past their end-of-life. Devices using an expired OS are more vulnerable to malware, and agency data are at greater risk of unauthorized access.

2.3 Does the organization have an enterprise deviation handling process and is it integrated with the automated capability. – No

The Department has issued policy creating an enterprise deviation handling process; however, it is not integrated with an automated solution.

2.3.1 Is there a process for mitigating the risk introduced by those deviations? – Yes

No exception noted. The Department has issued policy to ensure the risks introduced by identified deviations are mitigated.

S3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? – Yes

Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). – Yes

No exception noted. We found that the Department's current policy was substantially compliant and procedures at the two agencies we reviewed were in compliance with NIST SP 800-53.

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). – Yes

No exception noted. We found that all agencies reviewed identified all users, including Federal employees, contractors, and others who access organization systems.

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary. – Yes

No exception noted. Currently, the Department requires agencies to implement multi-factor authentication for all forms of remote access to agency information systems.³⁶ We found that two out of two sampled agencies reviewed by OIG had properly implemented multi-factor authentication.

3.1.4 If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). – Yes

No exception noted. We found that two of two agencies reviewed by OIG used multi-factor authentication linked to the Department's PIV credentials program.³⁷

3.1.5 Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). – Yes

No exception noted. We found that two of two agencies adequately planned for the implementation of PIV cards for logical access in accordance with government policies.

3.1.6 Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). – Yes

No exception noted. We found that two of two agencies adequately planned for the implementation of PIV cards for physical access in accordance with government policies.

3.1.7 Ensures that the users are granted access based on needs and separation-of-duties principles. – No

OIG testing found no exceptions in granting access based on user needs and separation-of-duties in the agencies we reviewed. However, both an agency contractor review found issues and an agency self-reported a problem in this area. As a result, accounts have excessive privileges which may result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

³⁶ DR 3505-003, *Access Control Policy* (August 11, 2009). Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government PIV card and the DoD common access card.

³⁷ The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12* (HSPD-12), originally issued in August 2004, requires Federal agencies to develop and deploy for all of their employees and contract personnel a PIV credential which is used as a standardized, interoperable card capable of being used as employee identification and allows for both physical and information technology system access.

3.1.8 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts). – Yes

No exception noted. We found that all agencies reviewed identified devices with Internet Protocol (IP) addresses that were attached to their network and were capable of distinguishing these devices from users.

3.1.9 Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) – Yes

No exception noted. We found that all agencies reviewed identified all user and non-user accounts.

3.1.10 Ensures that accounts are terminated or deactivated once access is no longer required. – No

OIG found that one agency reviewed did not ensure that accounts were terminated or deactivated once access was no longer required. For example, we found nine separated users in one agency that still had active accounts. In addition, two of six agencies self-reported deficiencies in this area. The agencies were not properly terminating users when access was no longer required, which could result in the unauthorized access, misuse, disclosure, disruption, modification, or destruction of information.

3.1.11 Identifies and controls use of shared accounts. – Yes

No exception noted. We found that all agencies reviewed did not use shared accounts.

3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.

No additional information was provided.

S4: Incident Response and Reporting

4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1). – No

We found the Department had developed policy and procedures for incident handling. However, we found that Departmental policy³⁸ did not include all NIST required elements and the procedures were not in compliance with USDA's current practices and thus were outdated.³⁹ Our review of two agencies found that both agencies had developed procedures but these procedures were not up-to-date with USDA's current incident processes.

In the FY 2011 FISMA report, OIG recommended that the Department update their incident handling procedures to reflect current practices. However, we found the Department's procedures were still outdated. This recommendation has reached management decision but has exceeded the estimated completion date of September 30, 2012.

4.1.2 Comprehensive analysis, validation and documentation of incidents. – No

Our review found that 14 of 78 incidents were not handled in accordance with Departmental procedures.⁴⁰ Based on our overall sample results, we estimate that 300 incidents (18 percent) were not handled in accordance with Departmental procedures.⁴¹

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). – No

US-CERT requires USDA to notify it of incidents within specified timeframes, based on the category of the incident.⁴² We reviewed a statistical sample of incidents and found that USDA had not reported 8 of 78 incidents to US-CERT within the required timeframe, 4 of which were the result of lost or stolen devices that were not promptly reported to the Department. Based on our overall sample results, we estimate that 171 incidents (10 percent), were not reported to US-CERT as required.⁴³ For example, US-CERT requires actual or potential personally identifiable information incidents to be reported within one hour, which includes lost or stolen equipment;

³⁸ DM 3505-005, *Cyber Security Incident Management Policy* (October 31, 2013).

³⁹ NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide* (August 2012).

⁴⁰ We based our sample size on a 30 percent error rate and a desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 78 incidents for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

⁴¹ We are 95 percent confident that between 158 (9 percent) and 442 (26 percent) incidents were not handled in accordance with departmental procedures. Additional sample design information is presented in Exhibit B.

⁴² US-CERT provides response support and defense against cyber-attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners. US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. NCSD was established by DHS to serve as the Federal Government's focal point for cyber security coordination and preparedness.

⁴³ We are 95 percent confident that between 59 (4 percent) and 284 (17 percent) incidents in fiscal year 2014 were not reported to US-CERT as required. Additional sample design information is presented in Exhibit B.

however, we found that an agency did not report a lost equipment incident to the Department (to forward to US-CERT) for 23 days.⁴⁴

4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61). – Yes

No exception noted. We found incidents were reported to law enforcement as required.

4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61, and OMB M-07-16, M-06-19). – No

Departmental procedures require that, if an incident remains open for more than 30 days, the agency is required to open a POA&M. However, we found 2 of 78 incidents that were not resolved in a timely manner, and no POA&M was created. Additionally, we reviewed incidents to determine if appropriate actions were taken for the resolution of the incident, and we identified 4 of 78 incidents which had inadequate remediation actions for closure.

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. – No

We verified with the Department that no changes had been made to their program in order to track and manage risks in a virtual/cloud environment. USDA lacks the ability to track cloud traffic, the cloud email system does not have a deployed DLP solution, and the service agreement between USDA and its cloud service provider does not include the appropriate detail outlining the roles and responsibilities for each party.⁴⁵

In the FY 2012 FISMA audit, we recommended that USDA modify the service agreement between the Department and the email cloud service provider to incorporate appropriate detail, outlining the roles and responsibilities of each party pertaining to incident response and reporting. Additionally, the Department needs to work with the cloud provider to gain visibility into USDA's email system allowing the Department to view/monitor network traffic in the cloud system. We conducted follow-up testing pertaining to the FY 2012 audit recommendation; however, no updates were provided by OCIO. Because the audit recommendation remains open, we concluded no updates pertaining to the contract have occurred.

Also, a Federal initiative, the Federal Risk and Authorization Management Program (FedRAMP), effective June 2014, requires agencies and cloud service providers to stipulate any specific incident reporting requirements, including who to notify and how to notify the agency.⁴⁶

⁴⁴ Lost equipment is defined as a lost or stolen laptop, smartphone, or other electronic device that is issued to USDA employees for performance of the employees' day-to-day responsibilities.

⁴⁵ DLP is the ability "to detect inappropriate transport of sensitive information. Examples of sensitive content are personal identifiers (e.g. credit card or Social Security numbers) or corporate intellectual property."

⁴⁶ The FedRAMP program supports the U.S. Government's objective to enable U.S. Federal agencies to use managed service providers that enable cloud computing capabilities. The program is designed to comply with FISMA.

USDA's current cloud service providers were required to become compliant by June 2014. However, another audit conducted during FY 2014 found that the Department's cloud service providers were not all FedRAMP compliant, as required by OMB.

4.1.7 Is capable of correlating incidents. – No

Based on our review, we determined that, although the Department has the capability to monitor and correlate incidents for incident response and reporting within USDA, the current security tools do not see or capture all network traffic.

In the FY 2011 and 2012 FISMA reports, OIG recommended the Department deploy adequate resources to monitor and configure new security tools and then adequately report and close the related incidents. Management decision has been reached on the FY 2012 recommendation but has not been reached on the FY 2011 recommendation. Final action has not been reached for either recommendation and both have exceeded their estimated completion date of September 30, 2013.

4.1.8 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). – Yes

No exception noted. Although the Department is not capable of correlating and monitoring incidents in a cloud environment (as noted in 4.1.7), we found that it has continually improved in overall incident management. Therefore, we concluded that it has sufficient incident detection and monitoring coverage.

4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

No additional information to provide.

S5: Risk Management

5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – No

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

5.1.1 Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. – No

The Department has a finalized risk management policy and procedures, but the procedures lack some required elements. For example, the procedures are missing guidance for an authorization termination date. This date is established by the authorizing official to indicate when the security authorization expires.⁴⁷ Without accessible procedures, the Department does not have a consistent and effective approach to risk management that is applied to all risk management processes and procedures.

In the FY 2011 FISMA report, OIG recommended the Department develop a risk management policy and associated procedures that fully comply with NIST. Management decision has been reached but OCIO has exceeded the estimated completion date of September 30, 2013.

5.1.2 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev.1. – No

The Department has not developed an organization-wide risk management strategy that addresses risk from an organizational perspective. According to OCIO officials, funding was reduced for the team responsible for the development and implementation of the governance project, which included the RMF strategy.

5.1.3 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1. – No

As noted in questions 5.1.1 and 5.1.2, the Department does not have adequate procedures, a governance structure, or an organizational risk management strategy. Therefore, it has not defined the risks from a mission and business process perspective in order to address them from an organizational perspective.

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1. – No

As noted in questions 5.1.1 and 5.1.2, the Department does not have adequate procedures, a governance structure, and an organizational risk management strategy. Therefore, officials have not defined the information system risks and the steps necessary to address them from a mission and business perspective.

⁴⁷ USDA *Six Step Risk Management Framework Process Guide* (December 2012). NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010), states that organizational officials must identify the resources necessary to complete the risk management tasks described in this publication and ensure that those resources are made available to appropriate personnel.

5.1.5 Has an up-to-date system inventory. – No

The Department does not have an up-to-date system inventory. We found 23 contractor systems not recorded in the CSAM system.⁴⁸ Currently, there is no way for USDA to ensure that all systems are recorded in CSAM and that USDA has an accurate inventory.

5.1.6 Categorizes information systems in accordance with government policies. – No

We generated a report from CSAM which identified the impact level for each of the Department's systems. The report included the impact levels for confidentiality, integrity, and availability, which were categorized as high, moderate, and low.⁴⁹ For instance, if any one of the impact levels is high then the system's categorization must be high. We compared the generated report to NIST's recommended categorization levels and found 18 of 239 systems were not properly categorized.⁵⁰ These systems had a lower categorization rating than was recommended, without adequate justification.⁵¹ NIST requires that any adjustments to the recommended impact levels be documented and include justification for the adjustment.

5.1.7 Selects an appropriately tailored set of baseline security controls. – No

NIST SP 800-53 recommends a set of minimum baseline security controls to be implemented based on a system's overall categorization. The lower the categorization level, the fewer required controls. Therefore, the incorrect categorization noted in 5.1.6 led to inadequate controls being implemented for those 18 systems. NIST SP 800-60 states that an incorrect information system impact analysis can result in the agency either overprotecting the information system (thereby wasting valuable security resources), or under protecting the information system and placing important operations and assets at risk.

5.1.8 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. – No

As noted in 5.1.6, the incorrect categorization noted in 5.1.7 led to inadequate controls being implemented for 18 systems.

⁴⁸ CSAM is a comprehensive system developed by the Department of Justice, which can help in achieving FISMA compliance. CSAM provides a vehicle for the Department, agencies, system owners, and security staffs to (1) manage their system inventory, interfaces, and related system security threats and risks; (2) enter system security data into a single repository to ensure all system security factors are adequately addressed; (3) prepare annual system security documents, such as security plans, risk analyses, and internal security control assessments; and (4) generate custom and predefined system security status reports to effectively and efficiently monitor each agency's security posture and FISMA compliance. This includes agency-owned systems or those operated by contractors on the agency's behalf.

⁴⁹ FISMA (44 U.S.C. Section 3542) defines integrity as guarding against improper information modification or destruction, and includes ensuring information on repudiation and authenticity. Confidentiality is defined as preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Availability is defined as ensuring timely and reliable access to and use of information.

⁵⁰ Systems inventory as of September 3, 2014.

⁵¹ NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Vol. 1 (August 2008).

5.1.9 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. – No

We found that security controls were not implemented correctly. Specifically, systems' security controls did not include sufficient support for implementation. For example, for 10 of 10 systems reviewed, the controls involving security awareness training, incident response, or program management were described as inherited. However, these controls could not be inherited. The Department requires the agencies to develop specific procedures on how the organization will implement these types of controls.⁵²

5.1.10 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. – No

The Department does not authorize information system operation based on a determination of the risk to organizational operations and assets. We found 5 operational systems with no ATO, and 50 operational systems with expired ATOs.⁵³ This occurred because the Department felt that all 55 systems needed to be operational for business needs.

In the FY 2012 FISMA report, OIG recommended that the Department verify that all systems have the proper ATO prior to implementation. Management decision has been reached but OCIO has exceeded the estimated completion date of September 30, 2013.

5.1.11 Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. – No

NIST SP 800-53 states that the organization will assess the security controls in an information system as part of the testing/evaluation process. However, as noted in 1.1.6, we identified 5 of 33 systems where ongoing assessments of selected security controls had not been performed in FY 2014.

5.1.12 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. – No

As noted in 5.1.1-5.1.4, the Department does not have adequate procedures, a governance structure, or an organizational risk management strategy with defined risks in place. Therefore, we were unable to determine if the information-system-specific risks were communicated to appropriate levels of the organization.

⁵² USDA *Six Step Risk Management Framework Process Guide* (December 2012).

⁵³ Total number of systems generated out of CSAM as of June 30, 2014.

5.1.13 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). – Yes

No exception noted. The Department briefs appropriate personnel through weekly activity reports.

5.1.14 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks. – Yes

No exception noted. The RMF guide prescribes the active involvement of appropriate personnel.

5.1.15 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, 800-37). – No

The SSPs we reviewed were inadequate and not in accordance with Government policies.⁵⁴ We found 10 of 10 SSPs did not meet the minimum security requirements required by NIST SP 800-53. Specifically, these systems' security controls did not include sufficient support for implementation. For instance, we found controls that had not been assessed and the agencies did not have evidence supporting why the controls were not assessed.

We also reviewed 10 of the Department's SARs and found that all 10 did not meet the minimum security required by NIST SP 800-37.⁵⁵ Specifically, NIST SP 800-37 requires a SAP to be included with the SAR, which provides the objectives for the security control assessment and a detailed roadmap of how to conduct the assessment. During our review we found that all 10 SAPs that had fully completed the A&A process had not been approved or authorized. As a result, USDA cannot be assured that all system controls had been documented and tested, and that the systems were operating at an acceptable level of risk.

As noted in 7.1.6, USDA's POA&Ms did not meet Federal guidelines.

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. – No

During our review of SSPs, we found 2 of 10 systems did not adequately define or explain the system boundaries. Unclear boundaries can lead to confusion over responsibility for system components.

⁵⁴ NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems* (February 2006), requires the SSP as part of the A&A documentation. It provides an overview of the security requirements of the system and describes the controls in place (or planned) for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system.

⁵⁵ The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the SAR.

5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.

No additional information to provide.

S6: Security Training

6.1 Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). – Yes

No exception noted. We determined the Department and two of two agencies' security awareness policies⁵⁶ and procedures met all the requirements outlined in NIST SP 800-53 for FY 2014.⁵⁷

In the FY 2011 FISMA report, OIG recommended that the Department develop monitoring procedures to appropriately report the status of USDA employees being trained to meet their information security awareness needs. This recommendation reached management decision, but has exceeded the estimated completion date of September 30, 2013.

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities. – Yes

No exception noted. The Department published policy on October 22, 2013⁵⁸ and two of two agencies' policy and procedures for specialized security training were effective and fully developed in accordance with NIST SP 800-53 for FY 2014.⁵⁹

⁵⁶ DR 3545-001, *Information Security Awareness and Training Policy* (October 22, 2013).

⁵⁷ Departmental SOP-CPPO-018, *Information Security Awareness Training* (April 21, 2011).

⁵⁸ DR 3545-001, *Information Security Awareness and Training Policy* (October 22, 2013).

⁵⁹ NIST SP 800-53 requires the organization to provide basic security awareness training to all users. Additionally, it requires the organization to identify and provide information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software with role-based specialized training related to their specific roles and responsibilities. The organization is to determine the appropriate content of security training and the specific requirements of the organization and the information systems to which personnel have authorized access.

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards. – Yes

No substantial exception noted. NIST SP 800-53 requires agencies to provide role-based training. OIG reviewed the training content for individuals of the two sampled agencies with significant information security responsibilities. We found 1,099 of 1,122 users (98 percent) had completed training that was appropriate for role-based training and was properly documented.

6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training. – Yes

No exception noted. NIST SP 800-53 requires agencies to document and monitor individual information system security training activities and to retain individual training records. During our review of two agencies, we found all users with login privileges had completed the annual security awareness training.

Although these two agencies have met the requirements, there is still an open recommendation. In the FY 2010 FISMA report, OIG recommended that the Department ensure its training repository is completely populated and all required personnel receive the training. This recommendation is still open and has exceeded the estimated completion date of August 30, 2011.

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. – Yes

No substantial exception noted. NIST SP 800-53 requires agencies to provide role-based training. Agencies are required to document and monitor individual information system security training activities and to retain individual training records. OIG reviewed the training content for individuals with significant information security responsibilities at the two sampled agencies. Our testing of 1,122 employees with significant security responsibilities found 1,099 employees (98 percent), from the 2 sampled agencies, had adequate role-based training to meet NIST requirements and had documented evidence of completing the specialized training.

6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53). – Yes

No exception noted. We found that the material for the security awareness training contained the appropriate content to meet NIST SP 800-53 and NIST SP 800-50 requirements.⁶⁰

⁶⁰ NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003).

6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

No additional information to provide.

S7: Plan Of Action & Milestones (POA&M)

7.1 Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. – Yes

No exception noted. The Department's security manual included a policy establishing a POA&M process for reporting IT security deficiencies and for tracking the status of remediation efforts. We reviewed this document and found it to include all required elements. The Department has also established procedures. Our review of the POA&M Standard Operating Procedure (SOP)⁶¹ determined it was updated to include OMB-outlined criteria.⁶² Additionally, testing at two agencies found that they have established POA&M procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. However, both agencies' procedures were missing a criteria element as required by OMB M-04-25.

7.1.2 Tracks, prioritizes and remediates weaknesses. – No

We found the Department's POA&M program tracks weaknesses. However, we identified 70 of 773 open and approved POA&Ms as of July 22, 2014, that did not have an identified priority level. Additional testing by contractors found that one of four agencies did not have a POA&M program that tracks, prioritizes, and remediates weaknesses. The Department uses CSAM as the central repository for POA&Ms, which includes tracking weaknesses, identifying priority levels, and housing all supporting documentation of remediation. In addition, the Department holds bi-weekly meetings with each agency to discuss POA&M status and any outstanding POA&M issues, in order to continually monitor agency progress.

⁶¹ Departmental Oversight and Compliance Division SOP-003, *Plan of Action and Milestones Management* (July 2013).

⁶² OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (August 23, 2004).

7.1.3 Ensures remediation plans are effective for correcting weaknesses. – No

OMB M-04-25 specifies that effective remediation of IT security weaknesses is essential to achieve a mature and sound IT security program, and to secure information and systems. It further states that a milestone should identify specific requirements to correct an identified weakness. To test the Department's remediation effectiveness, we reviewed a statistical sample of 52 POA&Ms that were closed during FY 2014, and found 13 were closed without documented remediation plans.⁶³ Based on our sample results, we estimate 213 POA&Ms (25 percent) were closed in FY 2014 with remediation actions that did not sufficiently address the identified weaknesses.⁶⁴ The Department also reviewed 97 POA&Ms and found that 50 were not acceptable due to insufficient documentation to support remediation, or closure procedures were not followed. Additional work by contractors identified one of two agencies did not ensure remediation plans are effective for correcting weaknesses.

In FY 2009 we recommended that the Department develop and implement an effective process to ensure POA&Ms are entered, tracked, and closed properly. Although this recommendation has reached final action and is closed, we continue to find that POA&Ms are not being closed properly.

7.1.4 Establishes and adheres to milestone remediation dates. – No

We found that 889 of the 3,094 (29 percent) milestones completed in FY 2014 were not completed by the planned milestone finish date. We found that milestone dates are being established, but the remediation dates are not always adhered to. Additional testing by contractors identified one of four agencies did not have a POA&M program which establishes and adheres to milestone remediation dates.

7.1.5 Ensures resources and ownership are provided for correcting weaknesses. – No

We found weaknesses that were not being remediated due to inadequate resources. We identified 274 delayed POA&Ms as of September 9, 2014. We determined 133 of the 274 POA&Ms were delayed due to inadequate resources. Additionally, 36 POA&Ms were delayed without providing an explanation. We also found that ownership was not assigned for 72 of 773 open POA&Ms as of July 22, 2014.

⁶³ We based our sample size on a 17 percent error rate and desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 52 POA&Ms for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

⁶⁴ We are 95 percent confident that between 113 (13 percent) and 314 (37 percent) of closed POA&Ms in FY 2014 had remediation actions that did not sufficiently address the identified weaknesses in accordance with Government policies. Additional sample design information is presented in Exhibit B.

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). – No

OMB requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been identified. The Department's SOP requires an agency to create a POA&M when an identified weakness cannot be remediated within 30 days. However, we found POA&Ms had not been created for the four FY 2013 FISMA Departmental audit recommendations. Also, we found that one agency was not creating POA&Ms for vulnerabilities that were outstanding for over 30 days.

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25). – Yes

No exception noted. OMB requires that POA&Ms include the estimated funding resources required to resolve the weakness. We found 57 of 858 (6.5 percent) POA&Ms did not have associated costs. The Department has made significant progress since FY 2011 when we found that 38 percent of the POA&Ms did not have associated costs. Therefore we consider the error rate in FY 2014 to be insignificant.

7.1.8 Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25). – Yes

No exception noted. OIG determined that the Department's POA&M program has established a process for program officials and contractors to report on remediation progress to the CIO on a regular basis, and that OCIO tracks and reviews POA&Ms at least quarterly. We found that the CIO receives monthly and weekly status reports for POA&Ms; additionally, the POA&M lead for the Department meets with agencies on a bi-weekly basis to discuss and address any issues identified during this review of their POA&Ms in progress.

7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

No additional information to provide.

S8: Remote Access Management

8.1 Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17). – No

Although the Department has a remote access policy,⁶⁵ our testing found it did not meet all NIST requirements.⁶⁶ There were two policy areas that were not addressed in the Departmental policy as outlined by NIST. One area was the administration of remote access servers and the other was the periodic reassessment of the telework device policies. Specifically, we found two of two agencies reviewed did not have a remote access policy, or procedures that were fully developed. This occurred because the agencies both deferred to their remote access service provider who failed to provide policy and procedures. As a result, inadequate security over remote access could result in the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

In the FY 2010 FISMA report, we recommended the Department develop a remote access and telework policy and procedures that fully comply with NIST. The recommendation was still open; OCIO has exceeded the estimated completion date of August 31, 2011.

8.1.2. Protects against unauthorized connections or subversion of authorized connections. – Yes

No exception noted. We found two of two agencies reviewed had programs protecting against unauthorized connections or subversion of authorized connections.

8.1.3. Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1). – Yes

No exception noted. Two of two agencies we reviewed were using the Departmental solutions for multi-factor authentication and for mobile device security.

8.1.4. Telecommuting policy is fully developed (NIST 800-46, Section 5.1). – No

As reported in item 8.1.1 above, the Department has a remote access (and telework) policy but our testing found it did not meet all NIST requirements. Specifically, we found one agency reviewed did not have a fully developed telecommuting policy. This occurred because the agencies' policy and procedures provided no detailed instructions for IT security. As a result, inadequate security over remote access could result in the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

⁶⁵ DM 3525-003, *Telework & Remote Access Security* (February 17, 2005).

⁶⁶ NIST SP 800-46 Rev. 1, *Guide to Enterprise Telework and Remote Access Security* (June 2009).

8.1.5. If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3). – Yes

No exception noted. We found that multi-factor authentication for remote access is required by Departmental policy, and also found two of two agencies reviewed had properly implemented multi-factor authentication.⁶⁷

In the FY 2010 FISMA report, we recommended that the Department complete the Departmental projects that will enforce multi-factor authentication and external media encryption. The recommendation has reached management decision but has exceeded the estimated completion date of September 30, 2011.

8.1.6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. – Yes

No exception noted. Multi-factor authentication for remote access was reviewed in item 8.1.5 above, and in that step we found that multi-factor authentication for remote access is required by Departmental policy, and also found two of two agencies we reviewed have multi-factor authentication properly implemented.

8.1.7. Defines and implements encryption requirements for information transmitted across public networks. – Yes

No exception noted. We found two of two agencies reviewed had defined and implemented encryption requirements for information transmitted across public networks.

8.1.8. Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. – Yes

No exception noted. We reviewed two agencies' remote access session time-out settings and found they were compliant with OMB M-07-16, and timed-out after 30 minutes of inactivity, after which re-authentication was required.⁶⁸

8.1.9. Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines). – No

Our review of 10 incidents involving lost or stolen remote access devices found 2 were not handled correctly and 5 were not reported appropriately. This occurred because the devices were not being wiped or disabled and the agency employees were slow to report the devices missing. As a result, inadequate handling of lost or stolen remote access devices could result in the unauthorized access, use, disclosure, modification, or destruction of information.

⁶⁷ DR 3505-003, *Access Control Policy* (August 11, 2009).

⁶⁸ OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).

8.1.10. Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53, PL-4). – Yes

No exception noted. We reviewed two agencies' rules of behavior agreements and found they were adequate in accordance with government policies.

8.1.11. Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6). – Yes

No exception noted. We reviewed two agencies' rules of behavior/user access agreements and found they were adequate in accordance with government policies.

8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.

No additional information to provide.

8.3. Does the organization have a policy to detect and remove unauthorized (rogue) connections? – No

While the Department and agencies were monitoring, detecting, and reporting unauthorized (rogue) connections, we found the Department had no policy requiring it. This occurred because the draft Departmental Logical and Physical Access Control Policy had not been issued. As a result, undetected unauthorized (rogue) connections increase the risk of unauthorized access, use, disclosure, modification, or destruction of information.

In the FY 2013 FISMA report, we recommended that the Department develop and implement a policy to detect and remove unauthorized (rogue) network connections. This recommendation has management decision but has exceeded its estimated completion date of September 30, 2014.

S9: Contingency Planning

9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1). – Yes

No exception noted. NIST SP 800-53 states that the organization must develop, disseminate, and review/update documented contingency planning policy. We found that the Department's contingency planning policy met these requirements.

In the FY 2010 FISMA report, OIG recommended that agencies develop effective contingency planning policy and procedures in accordance with NIST. This recommendation remains open with management decision but has exceeded the estimated completion date of September 30, 2011. The Department provided OIG with an updated contingency planning policy; however, it remained in draft form and was unimplemented at the end of FY 2014.

9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). – Yes

No exception noted. NIST states that conducting the BIA is a key element in a comprehensive information system contingency planning process.⁶⁹ The Department's guide on developing contingency plans requires that a BIA be completed, during the concurrency review, for each system.⁷⁰ We found two of two agencies reviewed by OIG have incorporated the BIA into their contingency plans.

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34). – Yes

No exception noted. We found that all contingency plans (32 of 32) had addressed the key information required by NIST SP 800-34. Both tested agencies used the same template for all of their contingency plans.

9.1.4 Testing of system specific contingency plans. – No

NIST SP 800-53 requires Federal agencies to test contingency plans for information systems, using organization-defined tests. This is done to determine the plans' effectiveness and the organization's readiness to execute the plans. We identified 100 of 266 systems⁷¹ for which USDA system contingency plans had not been tested or documentation had not been updated during FY 2014 as required.⁷²

9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). – No

NIST SP 800-53 requires the agency to have procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. We found that the documented business continuity and disaster recovery plans were not in place and cannot be

⁶⁹ NIST SP 800-34, *Contingency Planning Guide For Federal Information Systems* (May 2010).

⁷⁰ DM 3570-001, *Disaster Recovery and Business Resumption Plans* (February 17, 2005).

⁷¹ Systems Inventory as of October 1, 2014.

⁷² *USDA Contingency Plan Exercise Handbook*, Rev. 1.1 (February 2011).

implemented when necessary. For example, 30 of 49 statistically sampled system contingency plans did not have evidence of ongoing testing of the plan.⁷³ Based on our sample results, we estimate that 136 systems (61 percent) did not have evidence of ongoing testing.⁷⁴

In the FY 2010 FISMA report, OIG recommended that all required contingency planning documents be in CSAM, all required fields be properly populated, and that CSAM be periodically reviewed to ensure agency compliance. This recommendation remains open with management decision but has exceeded the estimated completion date of September 30, 2011. While the Department has made progress, during testing we found agencies that had not uploaded evidence of testing into the Department's official document repository, CSAM.

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). – Yes

No exception noted. NIST SP 800-53 requires Federal agencies to test the contingency plan to determine the effectiveness of the plan and their readiness to execute the plan. We found that all 81 of the systems we reviewed had documented training, testing, and exercise programs incorporated in their contingency plans.

9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. – No

NIST SP 800-53 requires Federal agencies to test contingency plans for information systems, review the contingency plan test results, and initiate corrective actions, if needed. As noted in 9.1.5, we found that there were 30 of 49 statistically sampled system contingency plans that did not have evidence of ongoing testing of the plan. We also identified 100 of 266 agency systems within the Department that did not have a testing date recorded in CSAM during FY 2014.

9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). – No

NIST SP 800-34 states that all recovery and reconstitution events should be well documented, including actions taken and problems encountered during recovery and reconstitution efforts. An after-action report, with lessons learned, should be documented and updated. Our review of 49 sampled systems from agencies in the Department found that 28 did not have after-action reports for the current year.

⁷³ We based our sample size on a 20 percent error rate and desired absolute precision of +/-10 percent, at the 95 percent confidence level. With these assumptions, we calculated a sample size of 49 contingency plans for review and selected them by choosing a simple random sample. Additional sample design information is presented in Exhibit B.

⁷⁴ We are 95 percent confident that between 108 (49 percent) and 164 (74 percent) systems did not have evidence of ongoing testing. Additional sample design information is presented in Exhibit B.

9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). – Yes

No material exception noted. NIST SP 800-53 requires alternate processing sites be established for information systems in case of a disaster. We statistically sampled 49 systems and found 48 of those systems met the requirement to provide an alternate processing site. One system in our sample did not have an alternate processing site.

9.1.10 Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53). – Yes

No exception noted. We found that 48 of 48 applicable systems from our statistical sample had alternate processing sites that were not subject to the same risks as the primary site.

9.1.11 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). – Yes

No exception noted. NIST SP 800-53 states that the organization should conduct user-level, system-level, and information system documentation backups. We found the one agency reviewed by OIG was performing backups in a timely manner.

9.1.12 Contingency planning that considers supply chain threats. – Yes

No material exception noted. We found 1 of 49 contingency plans in our statistical sample of Department systems that did not document or consider supply chain threats within the contingency plan. This occurred because the disaster recovery plan had not been completed. Based on our sample results, we estimate that less than 8 percent of the systems may not have complied with the requirement to consider supply chain or vendor threats.⁷⁵

9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

During our testing on another audit during the year, we noted a system that could not be recovered during a contingency plan exercise. This was due to a certain module that was not able to be brought back online.

S10: Contractor Systems

10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? – No

⁷⁵ We are 95 percent confident that less than 8 percent of the systems may not have complied with the requirement to consider supply chain threats. Additional sample design information is presented in Exhibit B.

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

10.1.1 Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. – Yes

No exception noted. We found that the Department had documented policies for information security oversight of systems operated on the organization's behalf by contractors or other entities, including USDA systems and services residing in the public cloud. However, the policy was not implemented until August 12, 2014.

10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines. (NIST SP 800-53: CA-2). (Base) – No

As noted in 10.1.3 and 10.1.4, we found operational contractor systems in CSAM with expired ATOs and systems with insufficiently documented interconnections; therefore, we determined that the Department's contractor systems program was not ensuring that security controls of contractor systems and services were effectively implemented and complied with organization guidelines. This occurred because the Department did not have policies or procedures for the oversight of contractor systems until August 2014. As a result, the lack of policies and procedures can cause confusion and inconsistencies among the agencies as to what is required of them. The lack of contractor system oversight could result in unauthorized access, use, disclosure, disruption, modification, or destruction of the systems.

10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in public cloud. – No

USDA's contractor systems program does not include a complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in the public cloud. We identified 31 USDA cloud systems and found 23 were not listed in USDA's inventory. In addition, we reviewed 19 operational contractor systems in CSAM and found 16 systems with no SSP or unsigned SSPs, 6 systems with expired ATOs, and 3 systems with insufficient interconnection documentation. This occurred because the Department did not have published policies and procedures until August 12, 2014.

10.1.4 The inventory identifies interfaces between these systems and organization-operated systems (NIST 800-53: PM-5). – No

We reviewed interconnection documentation for 19 operational contractor systems in CSAM and found that 3 had not adequately identified or documented their interfaces in CSAM. This occurred because the Department did not have a policy until August 12, 2014.

10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. – No

The Department's contractor systems program was not requiring appropriate agreements (e.g., memorandum of understanding (MOU), interconnection security agreement (ISA), contracts, etc.) for interfaces between contractor systems and those that it owns and operates. In item 10.1.4 above, we found three contractor systems that had not adequately identified or documented their interfaces in CSAM, which shows that the program was not sufficiently requiring the appropriate agreements.

In the FY 2012 FISMA report, we recommended the Department develop and implement an effective process for making sure interface connections are documented, and that ISAs accurately reflect all connections to the systems. The Department needs to review interfaces during the annual testing processes. The recommendation was open with management decision and exceeded USDA's estimated completion date of September 30, 2013.

10.1.6 The inventory of contractor systems is updated at least annually. – No

We found that the inventory reconciliation had not been completed within the last year. In the FY 2013 FISMA report, we recommended that the Department validate the system inventory annually. The recommendation remains open with management decision and an estimated completion date of September 30, 2014.

10.1.7 Systems that are owned or operated by contractors or entities, including organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. – No

As noted in 10.1.3, we found 16 systems with no SSP or unsigned SSPs, 6 contractor systems with expired ATOs, and 3 contractor systems with missing interconnection agreements. We also found 23 USDA cloud systems that were not in USDA's inventory.

10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

Nothing additional to report.

S11: Security Capital Planning

11.1 Has the organization established a security capital planning and investment program for information security? – Yes

Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. – Yes

No exception noted.

11.1.2 Includes information security requirements as part of the capital planning and investment process. – No

We reviewed the Exhibit 53B documentation submitted by USDA and the two selected agencies as part of the annual budgeting process.⁷⁶ Our testing determined USDA's security capital planning and investment program includes information security requirements as part of the capital planning and investment process; however, detailed testing determined two of the two agencies selected for testing could not provide adequate supporting documentation for the amounts submitted on their annual Exhibit 53B. This occurred because the agencies were unaware of the need to retain adequate supporting documentation used during the budgeting process once the budget was submitted. As a result, USDA lacks justification for the IT security costs portion of its budgetary request. One agency has since begun maintaining the supporting documentation for the budget request pertaining to the security capital planning and investment program.

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). – No

We reviewed the Exhibit 53B documentation submitted by USDA and the two selected agencies as part of the annual budgeting process. However, as noted in 11.1.2, detailed testing determined two of the two agencies selected could not provide adequate supporting documentation for the amounts submitted on their annual Exhibit 53B; therefore, a discrete line item for information security in organizational programming and documentation could not be supported.

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). – Yes

No exception noted.

11.1.5 Ensures that information security resources are available for expenditure as planned. – No

We reviewed the Exhibit 53B documentation submitted by USDA and the two selected agencies as part of the annual budgeting process. Our testing determined that the Exhibit 53B was prepared; however, as noted in 11.1.2, the agencies could not provide documentation that supported the amounts included on the Exhibit 53B. We determined the agency did not adequately plan when expending IT resources based on the Exhibit 53B because supporting documentation for the amounts was not maintained. This occurred because the agencies were unaware of the need to retain adequate supporting documentation used during the budgeting

⁷⁶ Agencies must provide IT investment information using the Agency IT Investment Portfolio (Exhibits 53A&B), *Guidance on Exhibit 53 and 300 – Information Technology and E-Government*, OMB (2012).

process once the budget was submitted. As a result, USDA lacks justification for the IT security costs portion of its budgetary request.

11.2 Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.

No additional items were noted in testing.

Exhibit B: Sampling Methodology and Projections

Objective:

This sample was designed to support OIG's FY 2014 FISMA audit. The objective of this audit was to evaluate the status of USDA's overall IT security program based on the following overarching criteria:

- effectiveness of the Department's oversight of agencies' IT security programs, and compliance with FISMA;
- agencies' systems of internal controls over IT assets;
- Department's progress in establishing a Departmentwide security program, which includes effective assessments and authorizations; and
- agencies' and the Department's POA&M consolidation and reporting process; and the effectiveness of controls over configuration management, incident response, IT training, remote access management, identity and access management, continuous monitoring, contingency planning, contractor systems, and IT capital planning.

FISMA Audit Universes and Sample Designs:

FISMA contains multiple areas pertaining to various areas of IT security. We incorporated statistical sampling in three FISMA areas. Each of those areas was represented by a different universe. The specific designs are summarized below.

1. Incident Response and Reporting

Universe:

The audit universe consisted of 1,670 incidents reported during FY 2014, as of July 24, 2014. Each incident had a unique identifier and was categorized based on incident type into 1 of 7 categories (coded as 0 to 6).

Sample Design:

Each incident category has specific procedures and timelines that must be met by OCIO and the agency. While standards differ among the categories, the standards fall into four common groups: checklist requirements, reporting requirements, timely resolution, and damage containment. Thus, each incident response can be assessed as "pass" or "fail" when compared to the criteria that specifically apply to that incident type. This allowed us to combine incident response performance results (pass or fail) for the mix of incident types.

We used a simple random sample of 78 incidents for review. The sample size was based on:

- 95 percent confidence level;
- +/-10 percent precision in an attribute testing scenario;
- A universe size of 1,670 units; and
- An average expected error rate of 30 percent, based on historical information.

A listing and counts of incidents within the different categories in our universe and sample are presented in Table 1.

Table 1: Sample design summary for Incident Response and Reporting

| Incident Category | Universe Count | Sample Count |
|---|----------------|--------------|
| Category 0 - Exercise/Network Defense Testing Count | 119 | 6 |
| Category 1 - Unauthorized Access Count | 342 | 10 |
| Category 2 - Denial of Service (DoS) Count | 4 | 1 |
| Category 3 - Malicious Code Count | 585 | 31 |
| Category 4 - Improper Usage Count | 47 | 1 |
| Category 5 - Scans/Probes/Attempted Access Count | 9 | 3 |
| Category 6 - Investigation Count | 564 | 26 |
| Total | 1,670 | 78 |

Results:

Results are projected to the audit universe of 1,670 incidents. Achieved precision, relative to the universe, is reflected by the confidence interval for a 95 percent confidence level. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.⁷⁷

The audit team tested a variety of criteria: whether the incidents were reported to US-CERT within the required timeframe; whether the proper checklist was completed, and if not, was still accepted by the ASOC; whether the completed Incident Identification Form was completed in its entirety; whether the required incident category checklist was completed; if incidents were open for over 30 days without a POA&M being created; and if the incidents were resolved to minimize further damage.

We developed a projection for whether or not incidents were reported to US-CERT within the requested timeframe, and an overall projection, which is based on the number of incidents found in our sample with at least one exception. We are reporting actual findings for the rest of the criteria tested.

⁷⁷ Scheaffer, Mendenhall, Ott, *Elementary Survey Sampling*, Seventh Edition, Brooks/Cole, ©2012.

Projections are shown in Table 2. The narrative interpretation of the results is presented below the table.

Table 2: Incident Response and Reporting Projections⁷⁸

| Criteria Tested | Estimate | Standard Error | 95 Percent Confidence Interval | | Coefficient of Variation | <u>Achieved Precision</u> ⁷⁹ |
|---|----------|----------------|--------------------------------|-------|--------------------------|---|
| | | | Lower | Upper | | |
| Estimated number of incidents not reported to US-CERT within the required timeframe | 171 | 56.375 | 59 | 284 | 0.329 | 7% |
| as a percent of universe | 10% | 3% | 4% | 17% | | |
| Estimated total number of incidents with at least one exception | 300 | 71.309 | 158 | 442 | 0.238 | 9% |
| as a percent of universe | 18% | 4% | 9% | 26% | | |

Based on our sample results, we estimate that:

- 171 incidents (about 10 percent of the universe) were not reported to US-CERT within the required timeframe. We are 95 percent confident that between 59 (4 percent) and 284 (17 percent) incidents were not compliant based on this criterion.
- 300 (about 18 percent of the universe) incidents were not handled in accordance with Departmental procedures. We are 95 percent confident that between 158 (9 percent) and 442 (26 percent) incidents had exceptions in one or more criteria tested.

2. Closed POA&Ms

Universe:

The universe consisted of 853 POA&Ms.

Sample Design:

We selected a simple random sample of 51 closed POA&Ms for review. We based our sample size on the following factors:

- 95 percent confidence level;
- +/- 10 percent precision in an attribute testing scenario;
- universe size of 853 units; and
- an average expected error rate of 17 percent based on historical information.

⁷⁸ All percentages used are rounded to the nearest whole number.

⁷⁹ Achieved precision is the difference between the estimate and the bounds divided by the size of the universe. For example: $(284-171)/1,670 = 7$ percent (rounded to the nearest whole number).

Results:

Results for all criteria are projected to the audit universe of 853 closed POA&Ms. Achieved precision relative to the audit universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.⁸⁰

Projections are shown in Table 3 below. The narrative interpretation of the results can be found below the table.

Table 3: POA&M (closed) Projections

| Criteria Tested | Estimate | Standard Error | 95 Percent Confidence Interval | | Coefficient of Variation | Achieved Precision |
|---|----------|----------------|--------------------------------|-------|--------------------------|--------------------|
| | | | Lower | Upper | | |
| Estimated number of closed POA&Ms reviewed that did not have effective remediation plans detailed in CSAM to correct the identified weakness. | 213 | 50.119 | 113 | 314 | .235 | 12% |
| as a percent of the universe | 25% | 6% | 13% | 37% | | |

Based on our sample results, we estimate that 213 POA&Ms in our universe (about 25 percent of the universe) did not have effective remediation plans detailed in CSAM to correct identified weaknesses. We are 95 percent confident that between 113 (13 percent) and 314 (37 percent) of the POA&Ms in the audit universe are non-compliant with this criterion.

3. System Contingency Planning

Universe:

We worked with three separate universes of systems. One universe consisted of 222 FISMA reportable systems from a variety of agencies that were documented in CSAM as of August 14, 2014. The other two universes consisted of reportable systems in the two agencies we reviewed. One agency's universe contained 37 systems and the other contained 12.

Each system is to have a contingency plan that contains very specific recovery information in the event of a disaster.

Sample Designs:

From the three universes mentioned above, we selected:

- A simple random sample of 49 from 222 systems used by various USDA agencies;
- A simple random sample of 20 out of 37 systems; and

⁸⁰ Op. cit., Scheaffer et al.

- A census of 12 systems.

The sample sizes were based on:

- 95 percent confidence level;
- +/-10 percent precision in an attribute testing scenario;
- universe size of 222 units; and
- an expected error rate of 20 percent, based on historical information.

Results:

We are using projections derived only from the sample representing the combined agencies’ universe of 222 systems. Actual findings, not statistical projections, are reported for the two agencies’ universes.

Results are projected to the audit universe of 222 systems. Achieved precision relative to the universe is reported for each criterion. The corresponding lower and upper bounds of the 95 percent confidence interval are also included. All projections are made using the normal approximation to the binomial as reflected in standard equations for a simple random sample.⁸¹

Projections are shown in Table 4. A narrative interpretation of the results is presented below the table.

Table 4: System / Contingency Planning Projections

| Criteria Tested | Estimate | Standard Error | 95 Percent Confidence Interval | | Coefficient of Variation | Achieved Precision |
|---|----------|----------------|--------------------------------|-------|--------------------------|--------------------|
| | | | Lower | Upper | | |
| Estimate of the number of systems with no evidence of ongoing testing | 136 | 13.782 | 108 | 164 | .101 | 12% |
| as a percent of universe | 61% | 6% | 49% | 74% | | |

- Based on our sample results, we estimate that 136 systems in our universe (about 61 percent of the universe) did not have ongoing testing or did not provide documentation of testing. We are 95 percent confident that between 108 (49 percent) and 164 systems (74 percent) are noncompliant with this criterion.
- In addition, we found 1 exception out of 49 when testing whether the Department’s systems complied with the requirement to consider supply chain threats. Based on this finding, we are 95 percent confident that less than 8 percent of the systems in our universe of 222 may not have complied with the requirement to consider supply chain threats.

⁸¹ Ibid.

To learn more about OIG, visit our website at
www.usda.gov/oig/index.htm

How To Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse

File complaint online: <http://www.usda.gov/oig/hotline.htm>
Click on Submit a Complaint

Telephone: 800-424-9121
Fax: 202-690-2474

Bribes or Gratuities
202-720-7257 (24 hours a day)



The U.S. Department of Agriculture (USDA) prohibits discrimination in all of its programs and activities on the basis of race, color, national origin, age, disability, and where applicable, sex (including gender identity and expression), marital status, familial status, parental status, religion, sexual orientation, political beliefs, genetic information, reprisal, or because all or part of an individual's income is derived from any public assistance program. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint of discrimination, write to USDA, Assistant Secretary for Civil Rights, Office of the Assistant Secretary for Civil Rights, 1400 Independence Avenue, SW., Stop 9410, Washington, D.C. 20250-9410, or call toll-free at (866) 632-9992 (English) or (800) 877-8339 (TDD) or (866) 377-8642 (English Federal-relay) or (800) 845-6136 (Spanish Federal-relay). USDA is an equal opportunity provider and employer.