United States Department of Agriculture

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act

Audit Report 50501-0015-12

October 2017

OFFICE OF INSPECTOR GENERAL

IMPORTANT NOTICE

This audit report contains sensitive information that has been redacted for public release, due to security concerns.

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act

Audit Report 50501-0015-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its IT security program and practices during FY 2017.

OBJECTIVE

The objectives of this audit were to evaluate the status of USDA's overall IT security program by evaluating the five Cybersecurity Framework security functions: Identify, Protect, Detect, Respond, and Recover, and to follow up on prior audit recommendations.

RECOMMENDS

The Department should continue its progress by issuing critical policy and completing actions on the 27 outstanding recommendations from the FYs 2009-2016 FISMA reviews.

REVIEWED

The scope was Department-wide, and we reviewed agency IT audit work completed during FY 2017. This audit covered seven agencies and offices operating 164 of the Department's 351 operational systems.

WHAT OIG FOUND

The Department continues to take positive steps to improve its information technology (IT) security posture, but many longstanding weaknesses remain. In FYs 2009-2016, OIG made 67 recommendations for improving the overall security of USDA's systems; 26 of the 27 open recommendations are overdue. We also noted that 40 prior recommendations have been closed, but our testing shows weaknesses still exist in 5 of those recommendations. We are not making any new recommendations because the recommendations made in prior FISMA reports address these security weaknesses.

Office of Management and Budget (OMB) considers "Managed and Measurable" an effective level of security. We found that the Department's maturity level to be at the "Defined" level. Based on OMB's criteria, the Department's overall score would indicate an ineffective level. The Department needs to implement the controls that it has defined. The Department and its agencies must cooperate to develop and implement an effective plan to mitigate security weaknesses identified in the prior fiscal year recommendations. We also noted that OCIO continues to implement its Continuous Diagnostic and Mitigation (CDM) project. This should expand USDA's continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, and prioritizing risk alerts.

Due to existing security weaknesses identified, 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. The Department agreed with our findings and stated it has developed corrective actions and project plans to address prior year recommendations.

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

October 31, 2017

The Honorable Mick Mulvaney
Director for the Office of Management and Budget
725 17th Street, NW.
Washington, D.C. 20503

Dear Mr. Mulvaney:

Enclosed is a copy of our report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act* (Audit Report 50501-0015-12), 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.

Phyllis K. Fong
Inspector General

Enclosure

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

DATE: October 31, 2017

AUDIT NUMBER: 50501-0015-12

TO: Gary Washington
Acting Chief Information Officer
Office of Chief Information Officer

ATTN: Megen Davis
Audit Liaison

FROM: Gil H. Harden
Assistant Inspector General for Audit
Gil H. Harden

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act

This report presents the results of our audit of the U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act (FISMA). The instructions for fiscal year (FY) 2017 FISMA reporting are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (IG FISMA Metrics), V1.0, dated April 17, 2017. This report contains our responses to the questions contained in these instructions. Your written response is included, in its entirety, as an attachment to the report.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audits. Portions of this report contains publicly available information and those sections will be posted to our website http://www.usda.gov/oig in the near future. A secured copy of the report in its entirety is being sent to the Director of the Office of Management and Budget.

Table of Contents

Background and Objectives

Background

Improving the overall management and security of information technology (IT) resources needs to be a top priority for the Department of Agriculture (USDA). Technology enhances the ability to share information instantaneously among computers and networks, but it also makes organization's 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 of the threats to the Department's critical systems and data.

On December 17, 2002, the President signed the e-Government Act of 2002 (Public Law 107–347), which includes Title III, Federal Information Security Management Act (FISMA 2002). Federal Information Security Modernization Act of 2014 (FISMA) required annual review and reporting requirements and 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.

On December 18, 2014, the President signed FISMA, which "amended FISMA 2002 to (1) reestablish the oversight authority of the Director of Office of Management and Budget (OMB) with respect to agency security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems."[1] According to FISMA, the Secretary must:

> develop and oversee implementation of operational directives requiring agencies to implement OMB standards and guidelines for safeguarding Federal information and systems from a known or reasonably suspected information security threat, vulnerability, or risk. It authorizes the Director of OMB to revise or repeal operational directives that are not in accordance with the Director's policies.[2]

FISMA also "directs the Secretary to consult with, and consider guidance developed by, the National Institute of Standards and Technology (NIST) to ensure that operational directives do not conflict with NIST information security standards."[3]

FISMA changes annual reporting requirements by directing that agencies:

> submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General of the Government Accountability Office (GAO). Reports are required to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.

[2] Ibid.

[3] Ibid.

> number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information.[4]

Further, it "requires OMB to ensure the development of guidance for evaluating the effectiveness of information security programs and practices."[5] As part of NIST's statutory role in providing technical guidance to Federal agencies, NIST works with agencies in developing standards.

FISMA requires that the head of each agency be responsible for:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- Complying with the requirements of NIST's related policies, procedures, and standards;
- Ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes; and
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing risk, determining the levels of information security, implementing policies to cost-effectively reduce risks, and periodically testing and evaluating security controls.

FISMA requires the Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. These evaluations (a) test the effectiveness of information security policies, procedures, and practices of a subset of agency information systems, and (b) assess the effectiveness of an agency's information security policies, procedures, and practices.[6]

The fiscal year (FY) 2017 IG FISMA reporting metrics[7] represent a continuation of work begun in FY 2016, when the IG metrics[8] were aligned with the five function areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. The FY 2017 IG FISMA Reporting Metrics completed this work by not only transitioning the Identify, Protect, and Recover functions to full maturity models, but by reorganizing the models themselves to be more intuitive. This alignment with the Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the Chief Information Officer

[4] Ibid.

[5] Ibid.

[6] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

[7] FY 2017 IG FISMA Reporting Metrics V1.0 (April 2017).

[8] FY 2016 IG FISMA Reporting Metrics V1.1.3 (September 2016).

(CIO) and IG metrics processes while providing agencies with a meaningful independent assessment of the effectiveness of their information security program.

Within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and risks. IGs assess each of these function levels against the listed criteria when assigning the agency's performance metric rating.

The five levels an agency can be assessed at in the maturity model are:

- Level 1: Ad-hoc - Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner;
- Level 2: Defined - Policies, procedures, and strategy are formalized and documented but not consistently implemented;
- Level 3: Consistently Implemented - Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking;
- Level 4: Managed and Measureable - Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes; and,
- Level 5: Optimized - Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The FY 2017 IG FISMA Reporting Metrics state that the "Managed and Measurable" level represents an effective information security program.

DHS' CyberScope website captures agencies' consolidated reporting results. Each Cybersecurity Framework security function area allots points to agencies based on their achievement of various levels of maturity. Ratings throughout the seven security function areas will be by a simple majority, where the most frequent level across the questions will serve as the area's rating. For example, if seven questions are in an area, and the agency receives "Defined" ratings for three questions and "Managed and Measurable" ratings for four questions, then the area rating is "Managed and Measurable." OMB and DHS ensure that area ratings are automatically scored when entered into CyberScope, and these scores rate the agency at the higher-level instance when two or more levels are the most frequently rated.

Objectives

The objectives of this audit were to evaluate the status of USDA's overall IT security program by evaluating the five Cybersecurity Framework security functions:

- **Identify**, which includes questions pertaining to Risk Management and Contractor systems;

- **Protect**, which includes questions pertaining to Configuration Management, Identity and Access Management, and Security and Privacy Training questions;
- **Detect**, which includes questions pertaining to Information Security Continuous Monitoring;
- **Respond**, which includes questions pertaining to Incident Response; and
- **Recover**, which includes questions pertaining to Contingency Planning.

This audit also had an objective to review corrective actions taken by Office of the Chief Information Officer (OCIO) to implement OIG's prior audit recommendations.

Section 1: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act

Findings and Recommendations

This report constitutes OIG's independent evaluation of USDA's IT security program and practices required by FISMA, based on the FY 2017 IG FISMA Reporting Metrics that use the maturity model indicators. IGs are required to assess the effectiveness of information security programs on a maturity model spectrum in which the foundation levels ensure that agencies develop sound policies and procedures and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. This evaluation reflects the Department's information security program's status based on the completion of 2017 FISMA testing.

USDA is a large, complex organization that includes 36 separate agencies and offices, most with their own IT infrastructure. Each of USDA's 36 agencies and offices, including OCIO, needs to be held accountable for implementing the Department's policies and procedures. Currently, FISMA scores are directly impacted by which agencies OIG selects for detailed testing and the state of the agency's information security environment. Therefore, an agency that earns a lower score will cause the Department's overall score to drop. Once compliance by all agencies is attained, FISMA testing results should be consistent, regardless of which agency is selected. This should also improve the Department's overall security posture.

OCIO continues to take positive steps for improving the Department's security posture. For instance, the Continuous Diagnostic and Mitigation (CDM) project the Department is participating in should expand its continuous diagnostic capabilities by increasing network sensor capacity, automating sensor collections, and prioritizing risk alerts. This is a positive step to attain a higher security capability. OMB considers Level 4 "Managed and Measurable" to be an effective level of security.[9] However, we found that the Department's maturity level for the five function areas to be at Level 2, "Defined." Based on these criteria, the Department's overall score would indicate an ineffective cybersecurity program. The Department needs to implement its controls and determine that they are operating as intended and are producing the desired outcome. Because of this new methodology, any historical comparison to past USDA FISMA scores would not be appropriate.

USDA senior management needs to continue its efforts in making sure each agency and office understands that how well it implements IT security directly influences USDA's overall security posture and FISMA score. The degree to which USDA, as a whole, complies with FISMA and other security guidance has a direct correlation to the security posture of each agency and office. For USDA to attain a secure and sustainable security posture, all 36 agencies and offices must consistently implement Departmental policy based on a standard methodology. When every

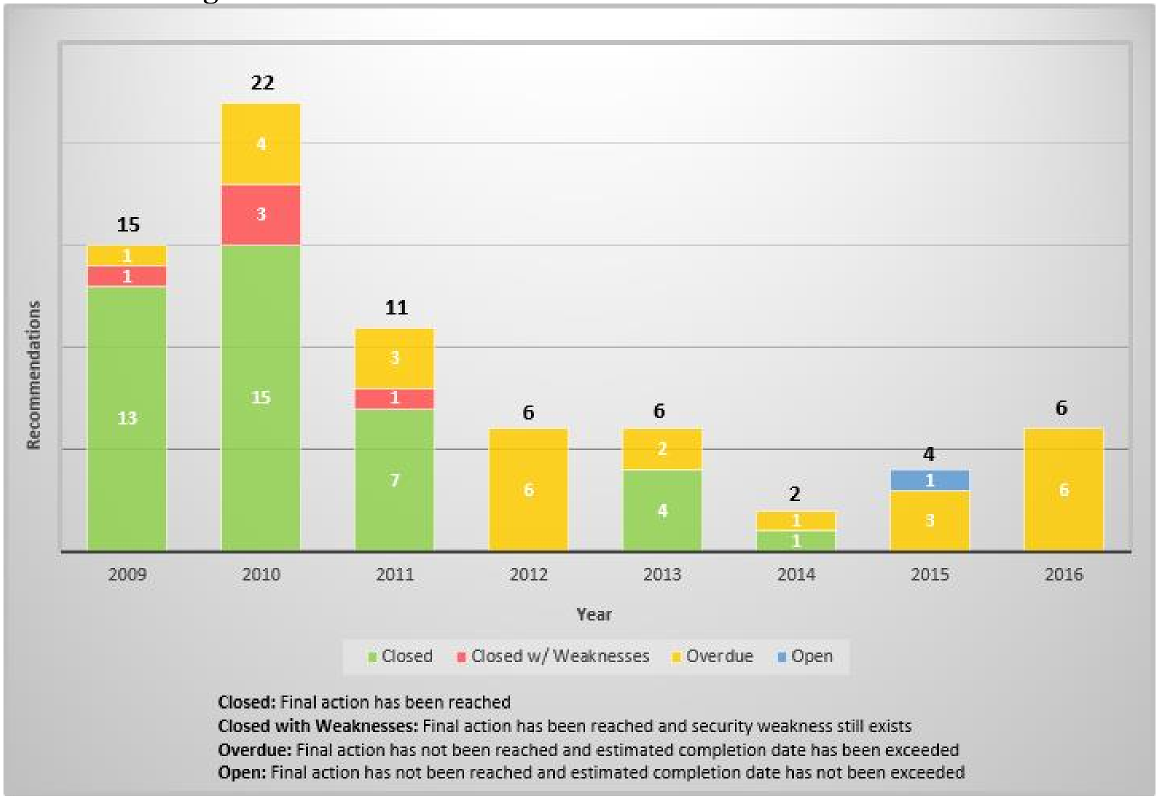
[9] According to the FY 2016 IG FISMA Reporting Metrics V1.0 (September 2016), security control effectiveness is the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

agency and office complies with USDA's policies, USDA, as a whole, will be FISMA compliant and, more importantly, will have a sustainable security posture.

We are not making any new recommendations this year because the recommendations made in prior FISMA reports address the security weaknesses noted this year. If corrective actions are effectively taken at the agency and Departmental levels, security weaknesses within the Department should be mitigated. The Department and its agencies must continue to work in cooperation to develop and implement an effective plan with objectives to mitigate security weaknesses identified in the prior fiscal year recommendations. The plan should prioritize tasks, define goals, and establish realistic timeframes that allow the Department to define and accomplish one or two critical objectives prior to proceeding on to the next set of priorities.

USDA is working to improve IT security, but many longstanding weaknesses remain. We continue to find that the Department has not implemented corrective actions in response to prior OIG recommendations. For FISMA audits from 2009 through 2016, OIG made 67 recommendations for improving the overall security of USDA's systems. Forty of the 67 recommendations have been closed, 1 open recommendation has not surpassed its implementation date, and the remaining 26 open recommendations are overdue. Our testing this year identified that security weaknesses still exist for five closed recommendations. The remaining outstanding recommendations address weaknesses related to these five recommendations; therefore, we maintain that no new recommendations are warranted.

FY 2009 through FY 2016 FISMA Recommendations Timeline



Closed: Final action has been reached
Closed with Weaknesses: Final action has been reached and security weakness still exists
Overdue: Final action has not been reached and estimated completion date has been exceeded
Open: Final action has not been reached and estimated completion date has not been exceeded

Due to existing security weaknesses identified, 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. Based on these outstanding recommendations, and the findings in this report, OIG concludes that the Department lacks an effective information security program.

Exhibit A contains OIG's responses to the OMB/DHS/Council of the Inspectors General on Integrity and Efficiency (CIGIE) FY 2017 FISMA security questions. These questions were defined on the DHS CyberScope FISMA reporting website. To address the FY 2017 IG FISMA Reporting Metrics, OIG reviewed annual agency self-assessments and various OIG audits throughout the year.[10] Since the scope of each review and audit differed, we could not use every review or audit to address each question. The following paragraphs summarize the key matters discussed in Exhibit A of this report.

Risk Management (Identify)

We found that the Department has established a risk management program that is operating at a Defined level. The Department has issued a guide[11] that addresses the six-step Risk Management Framework (RMF) process.[12] Although improvements have been made, we continue to find issues. The Department has not fully established an organization-wide risk management strategy that addresses risk from an organizational perspective or defined an information security architecture to meet a Consistently Implemented maturity level. For example, we reviewed 351 operational systems listed in Cyber Security Assessment Management System (CSAM)[13] and found 90 had invalid authorizations to operate (ATO).[14] In addition, there are currently five overdue recommendations relating to RMF, and one specifically regarding ATOs.[15] Closing out the FY 2016 FISMA recommendation to implement a

[10] Agency annual self-assessments are derived from OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016). 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.

[11] *USDA Six Step RMF Process Guide*, Revision 3.0 (December 2016).

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

[13] CSAM provides the USDA IT Security Program, program officials, and IT security managers with a web-based secure network capability to assess, document, manage, and report on the status of IT security risk assessments and implementation of Federal and USDA mandated IT security control standards and policies.

[14] The total number of operational systems with expired ATOs was generated out of CSAM as of Sept. 11, 2017. Departmental Regulation (DR) 3540-003, Security Assessment and Authorization (Aug. 12, 2014), defines ATO as the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

[15] Overdue Recommendation 14 and 19 from FISMA FY 2010; 4 and 5 from FISMA FY 2012; and 1 from FISMA FY 2016.

governance structure in accordance with the Risk Management Framework would help address establishing a strategy and an information security architecture.

Configuration Management (Protect)

The Department established and maintains a security configuration management (CM) program that is operating at the Defined maturity level. We found that the Department has established an adequate policy making standard baseline configurations available for all applicable operating systems; however, agencies have not followed the policy and have not met baseline standards when configuring workstations. For example, at one agency we found over nine percent of NIST's United States Government Configuration Baseline (USGCB) settings for Windows® workstations had deviations without the required documentation.[16] This has been an outstanding issue since the FY 2013 FISMA audit. The Department's CM policy is sound, but the agencies have not implemented the policy and the Department has not enforced it. Therefore, OIG has determined that the CM program is not operating at the Consistently Implemented maturity level and is not effective. In addition to the USGCB recommendation mentioned above, there are three additional overdue recommendations relating to CM that address compliance with policies.[17]

Identity and Access Management (Protect)

The Department has established an identity and access management program that is consistent with the Defined maturity level. For example, the Department has developed an account and identity management policy that is compliant with NIST standards and has adequately planned and implemented Personal Identity Verification (PIV) for non-privileged and privileged access in accordance with Government standards.[18] However, we found that 39 out of 685 separated employees did not have their user accounts disabled or deactivated. Therefore, the Department is not at the Consistently Implemented maturity level. There are currently one open recommendation and four overdue recommendations relating to Identity and Access Management.[19]

[16] DR 3520-002, Configuration Management (Aug. 12, 2014), states, "All deviations from USGCB settings shall be documented and submitted to the USDA Chief Information Security Officer (CISO) and be approved prior to implementation on agency and office production systems."

[17] Overdue Recommendation 2 from FISMA FY 2013; 2 from FISMA FY 2012; 4 from FISMA FY 2011; and 3 from FISMA FY 2010.

[18] The Executive Branch mandate entitled, *Homeland Security Presidential Directive 12* (HSPD-12) (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.

[19] Open Recommendation 4 from FISMA FY 2015; Overdue Recommendation 4 from FISMA FY 2013; and 1, 2, and 3 from FISMA FY 2016.

Security Training (Protect)

The Department has not established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. We found that the Department had policy[20] and procedures[21] that met all NIST requirements for annual security awareness training to meet the Defined level of maturity. However, we found that 1,649 out of 10,271 users had no security awareness training documented in FY 2017. Therefore, the Department is not at the Consistently Implemented maturity level. In 2016, OIG recommended the Department identify all users who need security awareness training, populate the training repository completely with those individuals, and ensure they receive the required training. This overdue recommendation remains open.[22]

Information Security Continuous Monitoring (ISCM) (Detect)

During our review, we found that USDA had established policy, procedures, and a Strategic Plan for ISCM strategy for continuous monitoring that satisfies the requirements for the maturity level of Defined.[23] However, the ISCM Strategic Plan had not been Consistently Implemented. The Department could not provide documentation of oversight or status reporting as stated in the ISCM Strategic Plan, and we found invalid ATOs as noted in the RMF section above. There are currently four prior recommendations still open relating to ISCM, and one open RMF recommendation specifically regarding ATOs. In addition, as noted above, completing the FY 2016 FISMA recommendation to implement a governance structure in accordance with the Risk Management Framework would also help improve ISCM oversight and system inventory accuracy.

Incident Response (Recover)

We found that the Department had an incident response and reporting program at the Defined maturity level. However, the Department's policy and procedures for meeting the laws, regulations, and standards of a comprehensive incident response program are not up to date and are currently only in draft. The procedures have been in draft since 2011. To alleviate delays in USDA’s overall policy approval process when issuing updated policies, in August 2017, the CIO delegated policy approval process authority to the Office of Information Security, Chief Information Security Officer. This should allow OCIO to issue policies more timely. Additionally, in FY 2018, OCIO has engaged an independent verification and validation organization to perform comprehensive process improvement of the cybersecurity and risk management policy development and approval process to enhance service and customer experience, streamline and/or reduce the process steps, and shorten the time to develop and

[20] DR 3545-001, *Information Security Awareness and Training Policy* (Oct. 22, 2013).

[21] Departmental SOP-CPPO-018, Information Security Awareness Training Standard Operating Procedures (Apr. 21, 2011).

[22] Overdue Recommendation 2 from FISMA FY 2016.

[23] *USDA Information Security Continuous Monitoring Strategic Plan*, Version 1.9 (Apr. 26, 2017).

approve a cybersecurity policy. Without adequate and up-to-date Departmental policy and procedures, agencies may not have sufficient resources and guidance when implementing their incident response program to meet the Consistently Implemented maturity level. There are currently three overdue recommendations relating to Incident Response that address the policy and procedure updates.[24]

Contingency Planning (Recover)

The Department established policies and procedures for an enterprise-wide business continuity/disaster recovery program and is operating at the Defined maturity level. However, we found those policies and procedures were not Consistently Implemented. For example, we found 22 of the 60 systems reviewed did not have current contingency plans and 44 of the 60 systems did not have the required annual contingency plan testing performed in at least 1 of the last 3 years.[25] There is one closed recommendation related to contingency plan testing that we continue to find as an issue.[26] Completing action on the FY 2016 FISMA recommendation to implement a governance structure in accordance with the Risk Management Framework would help to ensure that system contingency plans are tested at least annually.[27]

As noted above, we are not making any new recommendations this year. There are 27 recommendations from FISMA reports from 2009 through 2016 that have not yet been closed. If the agreed to corrective actions to close out the recommendations are no longer achievable due to budget cuts or other reasons, then OCIO needs to update those corrective action plans and request a change in management decision, in accordance with Departmental guidance.

[24] Overdue Recommendation 5 from FISMA FY 2011; 3 from FISMA FY 2012; and 2 from FISMA FY 2014.

[25] DR 3571-001, *Information System Contingency Planning and Disaster Recover Planning* (June 2016), states that contingency plans shall be tested at least annually.

[26] 50501-0002-IT FISMA FY 2010- Recommendation 17 states: “Ensure that all required contingency planning documents are in CSAM and all required fields are properly populated. This should include recovery strategies, plans, and procedures, as well as testing, training, and exercise results. Periodically review CSAM to ensure agency compliance.”

[27] Overdue Recommendation 1 from FISMA FY 2016.

Scope and Methodology

The scope of our review was Department-wide and included agency IT audit work completed during FY 2017. Audit fieldwork was performed from April 2017 through October 2017. Work was conducted at offices in Washington, D.C., and Kansas City, Missouri. Additionally, we included the results of IT control testing and compliance with laws and regulations performed by agency self-assessments. In total, our FY 2017 FISMA audit work covered seven agencies and offices:

- Animal and Plant Health Inspection Service
- Economic Research Service
- Forest Service
- OCIO
- Office of the Chief Financial Officer
- Rural Development
- Risk Management Agency

As of September 11, 2017, these agencies and offices operated 164 of the Department's 351 operational systems.

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

- Gathered the necessary information to address specific reporting requirements outlined in the FY 2017 IG FISMA Reporting Metrics.
- Tested specific FISMA requirements at the Department and selected agencies and summarized our results.
- Interviewed appropriate officials to gather the necessary information, including self-assessments and supporting documentation, to address the specific reporting requirements outlined in FY 2017 IG FISMA Reporting Metrics. 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 audit reports.
- Performed non-statistical sampling for testing where appropriate. Specifically, we selected 20 of 1,424 security incidents reported between October 1, 2016 and May 31, 2017 and ensured at least 1 incident per category was sampled. We selected 40 of 1,200 closed Plan of Action and Milestones (POA&M) with a Workflow Status Date between October 1, 2016 and August 23, 2017 and ensured at least 1 POA&M from each agency was sampled. We selected 31 of 305 FISMA reportable agency systems as of August 24, 2017 and ensured that at least 1 system per agency was sampled.
- Compared test results against NIST controls, OMB/DHS/CIGIE guidance, e-Government Act requirements, and Departmental policies and procedures to determine compliance.

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.

Abbreviations

AC	Access Control
AM	Asset Management
AT	Awareness and Training
ATO	Authorization to Operate
BE	Business Environment
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CA	Security Assessment and Authorization
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CIS	Center for Internet Security
CM	Configuration Management
CO	Communications
CP	Contingency Planning
CSAM	Cyber Security Assessment Management System
CSF	Cybersecurity Framework
CSIP	Cybersecurity Strategy and Implementation Plan
DE	Detect
DHS	Department of Homeland Security
DR	Departmental Regulation
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GISRA	Government Information Security Reform Act
GV	Governance
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
ICAM	Identity Credential and Access Management
ID	Identify
IG	Inspector General
IP	Information Protection Processes and Procedures
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	information technology
NARA	National Archives and Records Administration

NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
PR	Protect
PS	Personnel Security
RA	Risk Assessment
RC	Recover
RM	Risk Management Strategy
RMF	Risk Management Framework
SA	System and Services Acquisition
SANS	Sysadmin, Audit, Network, Security
SAT	Security Awareness Training
SDLC	System Development Life Cycle
SI	System and Information Integrity
SIEM	Security Information and Event Management
SP	Special Publications
TIC	Trusted Internet Connections
US-CERT	United States Computer Emergency Readiness Team
USDA	Department of Agriculture
USGCB	United States Government Configuration Baseline

The subsequent section of the report “Exhibit A” is not being publicly released due to the sensitive security content.

Exhibit A: Department of Agriculture Inspector General Section Report 2017 Annual FISMA Report

AGENCY'S
RESPONSE TO AUDIT REPORT

USDA

United States Department of Agriculture

Departmental
Management

Office of the Chief
Information Officer

1400 Independence
Avenue S.W.
Washington, DC
20250

TO: Steve Rickrode
Deputy Assistant Inspector General for Audit
Office of Inspector General

FROM: Gary S. Washington
Acting Chief Information Officer
Office of the Chief Information Officer

Digitally signed by FRANCISCO SALGUERO
DN: c=US, o=U.S. Government,
ou=Department of Agriculture,
cn=FRANCISCO SALGUERO,
0.9.2342.19200300.100.1.1=12001000021
809
Date: 2017.10.25 17:45:32 -04'00'

SUBJECT: U. S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2017 Federal Information Security Modernization Act Draft Audit Report

The Office of the Chief Information Officer (OCIO) appreciates the opportunity to review the draft OIG FY 2017 FISMA Audit Report. The OCIO has reviewed the report and agrees with Office of Inspector General (OIG) assessment of the Department's IT Security Program. OCIO has developed corrective actions and project plans to address the prior year OIG FISMA audit recommendations, and to document those actions sufficiently to achieve final action by the Office of the Chief Financial Officer (OCFO). A goal for closure of at least 50% of the overdue recommendations has been attached to the Chief Information Security Officer's (CISO) FY18 Performance Plan.

In order to strengthen the Department's cybersecurity, OCIO has developed a five-year strategic plan for cybersecurity. This plan incorporates the OIG findings and recommendations, the Executive Order on Cybersecurity (EO #13800) weaknesses, the Continuous Diagnostics and Mitigation (CDM) program milestones, and several other critical activities and operations into a cohesive master plan. In addition, OCIO will be working with all agencies at USDA to ensure that longstanding weaknesses and performance failures will be included and addressed.

If additional information is needed, please contact Megen Davis, OCIO Audit Liaison at (301) 504-4299 or via email at megen.davis@wdc.usda.gov.

cc: Christopher Lowe, OCIO, Chief Information Security Officer
Johanna Briscoe, DM, Chief of Staff
Lance Moore, OIG, Assistant Regional Inspector General
Jane Bannon, OIG, Director IT Audit Operations
Ted Kaouk, OCIO Chief of Staff
Brad Rounding, Director, OIS Security Operations Division
Doug Parry, Director, OIS Security Integration Division
Kimberly Hennings, Director, OIS Compliance, Audits, Policy & Enforcement Division
Megen Davis, OCIO Audit Liaison
Jane Davis, OCIO Executive Assistant
Cynthia Schwind, OIS FISMA Coordinator

Learn more about USDA OIG
Visit our website: www.usda.gov/oig/index.htm
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: www.usda.gov/oig/hotline.htm

Monday–Friday, 9:00 a.m.– 3:00 p.m. ET
In Washington, DC 202-690-1622
Outside DC 800-424-9121
TDD (Call Collect) 202-690-1202

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