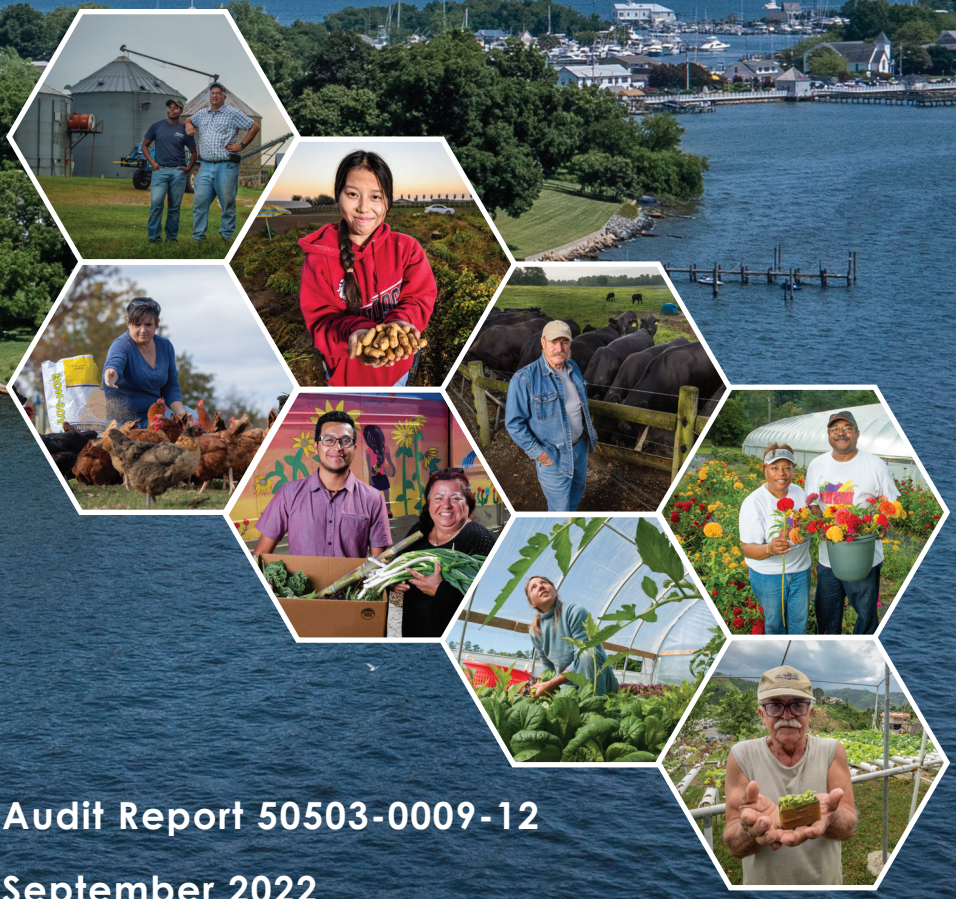
USDA OFFICE OF INSPECTOR GENERAL
U. S. DEPARTMENT OF AGRICULTURE

U.S. Department of Agriculture, Office of Chief Information Officer, Fiscal Year 2022 Federal Information Security Modernization Act



Audit Report 50503-0009-12

September 2022

IMPORTANT NOTICE

This audit report contains sensitive information that has been redacted for public release due to concerns about the risk of circumvention of law.

U.S. Department of Agriculture, Office of the Chief Information Officer, Federal Information Security Modernization Act of 2014 Audit Report for Fiscal Year 2021

Audit Report 50503-0009-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2022.

OBJECTIVE

The objective of this audit was to determine the effectiveness of USDA's information security program.

REVIEWED

We evaluated security controls in accordance with applicable legislation, standards and guidelines, presidential directives, OMB memorandums, and USDA policies and procedures. We selected three service centers under the purview of USDA OCIO. Of the service centers' 62 systems, we conducted system level testing for 8 USDA information systems.

RECOMMENDS

We recommend the Department: prioritize resources to implement NIST SP 800-53, Rev. 5; document and implement a process for transferring responsibility when the designated authorizing official (AO) changes; verify that all transferred AOs have transferred responsibility for the system or inherited controls; ensure that privileged user reviews are completed; verify controls to ensure that all privileged users are transferred to the identity management system; provide targeted personal identifiable information trainings more frequently; and design and implement a process to ensure documentation is retained.

WHAT OIG FOUND

The United States Department of Agriculture (USDA) continues to take positive steps to improve its information technology (IT) security posture, but many weaknesses remain. Out of 25 previously open recommendations identified during the fiscal year (FY) 2020 and FY 2021 Federal Information Security Modernization Act of 2014 (FISMA) performance audits, we determined USDA successfully closed 8 recommendations during our fieldwork that ended on June 30, 2022. We have also issued seven new recommendations based on security weaknesses identified in FY 2022.

The Office of Management and Budget (OMB) establishes standards for an effective level of security and considers "Managed and Measurable" to be a sufficient level. However, we found the Department's maturity level to be at the "Consistently Implemented" level. Based on OMB's criteria, the Department's overall score indicates an ineffective level of security. The Department and its agencies must develop and implement an effective plan to mitigate security weaknesses identified in the prior fiscal year recommendations.

USDA **OFFICE OF INSPECTOR GENERAL**
United States Department of Agriculture

DATE: September 27, 2022

AUDIT NUMBER: 50503-0009-12

TO: Gary S. Washington
Chief Information Officer
Office of the Chief Information Officer

ATTN: Megan Davis
Audit Liaison

FROM: Yarisis Rivera-Rojas
Acting Assistant Inspector General for Audit

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2022 Federal Information Security Modernization Act Audit

This report presents the results of the subject review. The instructions for fiscal year (FY) 2022 Federal Information Security Modernization Act (FISMA) are outlined in the Inspector General Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget Memorandum M-22-05 reporting guidance for FISMA dated December 6, 2021. This report contains our responses to the questions contained in these instructions. Your written response to the draft is included in its entirety at the end of the report. Corrective actions plans for the recommendations contained in the report should be provided to the Office of Inspector General within 60 days of this report date.

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of each management decision to prevent being listed in the Department's annual Agency Financial Report. For agencies other than OCFO, please follow your internal agency procedures in forwarding final action correspondence to OCFO.

We appreciate the courtesies and cooperation extended to us by members of your staff during our audit fieldwork and subsequent discussions. Portions of this report contain 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.

U.S. Department of Agriculture's Office of the Chief Information Officer Compliance with the Federal Information Security Modernization Act Audit for Fiscal Year 2022

September 26, 2022

kpmg.com

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

Chief Information Officer and Inspector General
U.S. Department of Agriculture
1400 Independence Ave., SW
Washington, DC 20250

U.S. Department of Agriculture's Office of the Chief Information Officer Compliance with the Federal Information Security Modernization Act Audit for Fiscal Year 2022

This report presents the results of our independent performance audit of the U.S. Department of Agriculture's (USDA or Department) information security program and practices for its information systems. We conducted our performance audit from May 9, 2022, through June 30, 2022, and our results are through the period of October 1, 2021, through June 30, 2022.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to determine the effectiveness of USDA's information security program. As such, we evaluated relevant security controls and processes referenced in the five Cybersecurity Function areas outlined in the Fiscal Year (FY) 2022 Core Inspector General (IG) Metrics, as specified in the Office of Management and Budget's (OMB) *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*. We responded to the FY 2022 Core IG FISMA Reporting Metrics and assessed the maturity levels on behalf of the USDA Office of Inspector General (OIG). (See Appendix II: FY 2022 IG FISMA Reporting Metrics). As part of our testing, we also followed up on the status of prior year recommendations.[1, 2]

[1] Audit Report 50503-0005-12, *Fiscal Year 2021 Federal Information Security Modernization Act*, Oct. 2021.
[2] Audit Report 50503-0003-12, *Fiscal Year 2020 Federal Information Security Modernization Act*, Oct. 2020.

Based on the maturity levels calculated in CyberScope,[3] we determined USDA's information security program was not effective as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines. According to FY 2022 Core IG Metrics, as specified in OMB *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*, a security program is considered effective if the majority of the FY 2022 Core IG Metrics are at least Level 4: Managed and Measurable. **Table 1** below depicts the maturity levels for the five Cybersecurity Functions we assessed for USDA's information security program.

Table 1: Maturity Levels for Cybersecurity Functions

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Assessed Maturity Level for USDA's Information Security Program
1. Identify Risk Management (RM) Supply Chain Risk Management (SCRM)	*1. Managed and Measurable (Level 4)* RM – Level 4 SCRM – Level 2
2. Protect Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)	*2. Defined (Level 2)* CM – Level 2 IAM – Level 5 DPP – Level 3 ST – Level 3
3. Detect Information Security Continuous Monitoring (ISCM)	*3. Consistently Implemented (Level 3)* ISCM – Level 3
4. Respond Incident Response (IR)	*4. Managed and Measurable (Level 4)* IR – Level 4
5. Recover Contingency Planning (CP)	*5. Consistently Implemented (Level 3)* CP – Level 3
Overall Maturity Level	**Consistently Implemented (Level 3)**
Overall Effectiveness	**Not Effective**

Source: CyberScope Appendix A: Scoring Maturity Model

During FY 2022, we tested security controls at the Department level and three Office of the Chief Information Officer (OCIO) service centers for a selection of eight systems. We identified and reported five findings (see Audit Recommendations and Findings) specific to the FY 2022 Core IG Metrics. The findings were identified in four of the five FISMA Cybersecurity Functions (Identify, Protect, Detect, and Respond) and in six of the nine FISMA Metric Domains (RM, SCRM, CM, IAM, ISCM, and IR).

We determined USDA's Department-wide and selected service centers' information security policies and procedures have not been updated to comply with NIST Special Publications (SP) 800-53, Revision

[3] CyberScope, operated by Department of Homeland Security (DHS) on behalf of OMB, is a web-based application designed to streamline Information Technology (IT) security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, IGs provide an independent assessment of effectiveness of an agency's information security program. USDA OIG must report its assessment results to DHS and OMB annually through CyberScope.

(Rev.) 5, *Security and Privacy Controls for Federal Information System and Organization*.[4] Additionally, we noted findings associated with the improper transition and designation of Authorizing Official (AO) duties, lack of recertification of privileged user accounts, and untimely reporting of a Personal Identifiable Information (PII) incident. We made seven recommendations related to these findings that should strengthen USDA's information security program if effectively addressed by management.

We also evaluated the implementation of recommendations identified during the FY 2020 and FY 2021 FISMA performance audits, during our field work that ended on June 30, 2022 we determined USDA successfully closed 8 recommendations and the issues did not recur during the performance audit period. (See Appendix III: Status of Prior Recommendations).

KPMG LLP (KPMG) cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of USDA, USDA OIG, DHS, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

September 26, 2022

[4] USDA Standard Operating Procedures (SOP) for RM Framework, SOP-3540-003, Volumes A to L, various dates.

Table of Contents

Background

KPMG LLP (KPMG) performed the fiscal year (FY) 2022 independent Federal Information Security Management Act of 2014 (FISMA) audit, under contract with the United States Department of Agriculture (USDA or Department) and on behalf of USDA Office of Inspector General (OIG), as a performance audit in accordance with Generally Accepted Government Auditing Standard (GAGAS). USDA OIG monitored our work to ensure we met professional standards and contractual requirements.

USDA relies extensively on information technology (IT) systems and resources to accomplish its mission. The IT systems and resources strengthen management and oversight of the Department's procurement, property, and finances to help ensure resources are used as effectively and efficiently as possible. Improving the overall management and security of IT resources and stakeholder information must be a top priority for the Department. While technology enables and enhances the ability to share information instantaneously among stakeholders through computers and networks, it also makes an 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 significant threats to the Department's critical systems.

Agency Overview

USDA's mission is to provide effective, innovative, science-based public policy leadership in agriculture, food and nutrition, nature resource protection and management, rural development, and related issues with a commitment to deliverable equitable and climate-smart opportunities.

Program Overview

USDA's Office of the Chief Information Officer (OCIO) operates within the Office of Secretary and has a mission of serving the information needs for USDA. OCIO will support achievement of USDA's diverse mission areas by offering agile, world-class technology solutions to its stakeholders and applying innovative approaches to recruiting and developing a highly skilled workforce. OCIO develops, delivers, and defends the business information technologies that empower every aspect of USDA's mission.

In support of OCIO's mission, services related to end-user support, data center operations, application development, and wide-area network telecommunications are provided to USDA agencies and staff offices by the following five service centers, all of which fall under the purview of OCIO: Information Security Center (ISC), Digital Infrastructure Services Center (DISC), Enterprise Geospatial Management Office, Client Experience Center (CEC), and Information Resource Management Center.

OCIO has five strategic goals in support of USDA's mission:

1. *Accelerate Digital Transformation:* Scale, modernize, and create innovative technology solutions that are based on customer needs.

2. *Drive Innovation in Support of the USDA Mission:* Advanced technologies are changing rapidly and increasing complexity. USDA will continue to drive innovation as it leverages advanced technologies to deliver services including drones, driverless tractors, remote sensing, augmented reality, and climate smart agriculture and forestry.
3. *Improve IT Organizational Agility with a Skilled Workforce:* Focus on building an agile organization to improve customer satisfaction. This will be achieved through a skilled and agile workforce that delivers results quickly, as well as through our processes for encouraging continuous feedback from customers and staff.
4. *Build Resilience into Everything We Do:* Apply the concept of cyber resiliency, which is defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources" to operations and cybersecurity capabilities.
5. *Enable Data-Driven Decision-Making:* Commit to building a culture that values data and promotes public data use through effective governance processes and robust data management practices that promote efficient and appropriate data use.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provide a mechanism for improved oversight of Federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment (1) included the reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing the risks and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

FISMA Inspector General Metrics and Changes from FY 2022

For FY 2022, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, DHS, the Federal Chief Information Officers, and Chief Information Security Officer (CISO) Council, developed the FY 2022 Core Inspector General (IG) Metrics[5] around five Cybersecurity Functions[6] outlined in the National Institute of Standards and

[5] OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines,* April 13, 2022.
[6] In its *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.0, NIST created Functions to organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities.

Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*[7] *(Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover*. The FY 2022 Core IG Metrics were chosen based on alignment with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, as well as OMB guidance provided to agencies to further the modernization of Federal cybersecurity. Subsequently, OMB provided the following guidance: *Moving the United States (U.S.) Government Toward Zero Trust Cybersecurity Principles* (M-22-09), *Multifactor Authentication and Encryption* (EO 14028), *Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31), *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01), and *Software Supply Chain Security & Critical Software* (Section 4 of EO 14028).

In addition, M-22-05 *Fiscal Year 2021–2022 Guidance on Federal Information Security and Privacy Management Requirements,* adjusted the timeline for the IG evaluation. Specifically, M-22-05 requires that the core group of metrics be evaluated annually and the remainder of the metrics be evaluated on a 2-year cycle, as agreed to by CIGIE, CISO Council, OMB, and the Cybersecurity and Infrastructure Security Agency.

The FY 2022 Core IG FISMA Metrics use the CIGIE maturity models for the nine FISMA Metric Domains:

- Risk Management (RM)
- Supply Chain Risk Management (SCRM)
- Configuration Management (CM)
- Identity and Access Management (IAM)
- Data Protection and Privacy (DPP)
- Security Training (ST)
- Information Security Continuous Monitoring (ISCM)
- Incident Response (IR)
- Contingency Planning (CP)

Table 2 outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domains.

[7] The President issued EO 13636, *Improving Critical Infrastructure Cybersecurity*, on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the EO calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and leading practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between the Government and the private sector, uses a common language to address and cost-effectively manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses.

Table 2: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FISMA Metric Domains within the FY 2022 Core IG FISMA Metrics

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	RM SCRM
Protect	CM IAM DPP ST
Detect	ISCM
Respond	IR
Recover	CP

IG FISMA Scoring

The ratings in the nine Domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a simple majority, where the most frequent level (mode) for the questions was the Domain rating. When responses are entered, the calculations were performed by CyberScope and determine the rating for each Domain and Function.

The maturity model has five levels: Level 1: Ad-hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. **Table 3** details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework Function. A security program is considered effective if a simple majority of the FY 2022 Core IG FISMA Metrics are at least Level 4: Managed and Measurable.

Table 3: Inspector General Assessed Maturity Levels

Maturity Level	Description
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 Measurable	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.
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.

Objective, Scope and Methodology

Objective

In accordance with FISMA, the objective of this performance audit was to determine the effectiveness of USDA's information security program. As such, we assessed relevant security controls and processes referenced in the five Cybersecurity Function areas outlined in the FY 2022 Core IG FISMA Metrics. We reviewed corrective actions taken by USDA to implement the prior FISMA performance audit recommendations. We also responded to the FY 2022 Core IG FISMA Metrics and assessed the maturity levels on behalf of USDA OIG.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2022 IG FISMA Reporting Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memorandums referenced in the reporting metrics; and USDA policies and procedures. We performed procedures to assess whether controls established by USDA's information security program were suitably designed, implemented, and operating effectively from both an entity-wide and service center-level perspective for those information systems selected in connection with our performance audit.

We selected three service centers under the purview of USDA OCIO, which were CEC, DISC, and ISC. Of the 62 systems pertaining to the three selected service centers, we took a representative selection and conducted system level testing for 8 USDA information systems (5 Government systems and 3 contractor systems).

Methodology

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our performance audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements, or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

We designed testing procedures for the purposes of assessing whether USDA controls were designed in accordance with relevant requirements and operated in a manner consistent with their intended design throughout the period under audit. When designing procedures to assess the operating effectiveness of manual controls, we applied a non-statistical random selection where the size of the population (i.e., the number of occurrences of the control) was a determining factor,

as described in the following paragraphs. **Table 4** below provides the frequency of control operation (population size) and the minimum selection size and the following considerations:

Table 4: Minimum selection size based on frequency of control operation (population size)

Frequency of control operation (Size of the population)	Minimum selection size
Annual (1)	1
Quarterly (2–4)	2
Monthly (5–12)	2
Weekly (13–52)	5
Daily (53–365)	15
Recurring Manual (multiple times/day) (>365)	25

The following approach was agreed upon with USDA OIG for conducting this performance audit and determining the maturity levels for each of the five Cybersecurity Functions and nine FISMA Metric Domains from the FY 2022 Core IG Metrics:

- We requested USDA management communicate its self-assessed maturity levels, where applicable, to confirm our understanding of the FISMA-related policies and procedures, guidance, structures, and processes established by USDA. The self-assessment helped us to plan our inquiries with management and understand the specific artifacts to evaluate as part of the FISMA performance audit.
- We performed test procedures over selected security controls performed by management and in-scope systems (where applicable), leveraging maturity Level 3 (Consistently Implemented) questions within the nine FISMA Metric Domains. If we identified findings associated with metrics that were tested in consideration of maturity Level 3 questions, we considered the nature of the identified finding(s) and assessed the maturity at Level 1 (Ad-hoc) or Level 2 (Defined) for the questions with responses indicating control failures.
- For metrics determined to be at maturity Level 3, we performed further procedures leveraging maturity Level 4 (Managed and Measurable) questions within the nine FISMA Metric Domains. If we identified findings associated with metrics that were tested in consideration of maturity Level 4 questions, we assessed the maturity at Level 3 for the questions with responses indicating control failures.
- For metrics determined to be at maturity Level 4, we performed further procedures leveraging maturity Level 5 (Optimized) questions within the nine FISMA Metric Domains. We performed these procedures to evaluate the design of the metrics. If we identified findings associated with metrics that were tested in consideration of maturity Level 5 questions, we assessed the maturity at Level 4 for the questions with responses indicating control failures.

Per the results of our test procedures, we input the maturity level for each of the 20 FY 2022 Core IG Metrics into the CyberScope reporting tool, which automatically calculated the Cybersecurity Function maturity levels based on the simple majority (mode) of the metric levels.

Our procedures included the following to assess the effectiveness of the information security program and practices of USDA:

- Inquiry of information system owners, Information System Security Officers, system administrators, and other relevant individuals to walk through each control process;
- An inspection of the information security practices and policies established by USDA;
- An inspection of the information security practices, policies, and procedures in use across USDA; and
- An inspection of artifacts to determine the design, implementation, and operating effectiveness of security controls at the program and system levels.

We performed our fieldwork from May 9, 2022, through June 30, 2022. Due to the coronavirus disease 2019 pandemic, all testing was performed remotely through virtual meetings, walkthroughs, and observations with representatives from USDA. During our performance audit, we met with OCIO and OIG remotely to discuss our findings.

Criteria

We focused our FISMA performance audit approach in consideration of Federal information security guidance developed by NIST and OMB. NIST Special Publications (SP) provide guidelines associated with the development and implementation of agencies' security programs. Federal agencies were required to update their security policies and procedures to comply with NIST SP 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53, Rev.5), as it superseded NIST SP 800-53, Rev. 4, effective September 23, 2021. We also leveraged a variety of USDA directives, manuals, standard operating procedures (SOPs), and other system-level guidance for information security.[8] For each finding detailed in the Audit Findings and Recommendations section, we included the relevant USDA, OMB, and/or NIST criteria.

[8] USDA Department-level directives, manuals, and other guidance for information security can be found via the USDA website at https://www.usda.gov/directives. Service center and system specific policy and procedures are stored in restricted locations.

Overall Results

We assessed the effectiveness of USDA's information security program on a maturity model spectrum where the foundational levels ensure that sound policies and procedures are designed and developed and the advanced levels capture the extent to which those policies and procedures have been implemented and operating effectively. The overall maturity of USDA's information security program is then calculated based on the average rating of the associated domains. Based on the maturity levels calculated in CyberScope, we determined USDA's information security program was not effective as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. A security program is considered effective if most of the FY 2022 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable. **Table 5** below depicts USDA maturity levels for the five Cybersecurity Functions.

Table 5: Maturity Levels for Cybersecurity Functions

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
1. Identify Risk Management (RM) Supply Chain Risk Management (SCRM)	*1. Managed and Measurable (Level 4)* RM – Level 4 SCRM – Level 2
2. Protect Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)	*2. Defined (Level 2)* CM – Level 2 IAM – Level 5 DPP – Level 3 ST – Level 3
3. Detect Information Security Continuous Monitoring (ISCM)	*3. Consistently Implemented (Level 3)* ISCM – Level 3
4. Respond Incident Response (IR)	*4. Managed and Measurable (Level 4)* IR – Level 4
5. Recover Contingency Planning (CP)	*5. Consistently Implemented (Level 3)* CP – Level 3
Overall Maturity Level	**Consistently Implemented (Level 3)**
Overall Effectiveness	**Not Effective**

Source: CyberScope Appendix A: Scoring Maturity Model

During FY 2022, we tested security controls at the Department-level and for a selection of three OCIO service centers and eight OCIO systems. We identified and reported five findings (see Audit Recommendations and Findings) specific to the FY 2022 Core IG Metrics. Findings were identified in four of the five FISMA Cybersecurity Functions (Identify, Protect, Detect, and Respond) and in six of the nine FISMA Metric Domains (RM, SCRM, ISCM, IAM, and IR). We also evaluated the implementation of recommendations from prior FISMA reports that remained open. Out of 25 previously open recommendations identified during the FY 2020 and FY 2021 performance audits, during our fieldwork that ended on June 30, 2022 we determined USDA successfully closed 8 recommendations and the issues did not recur during the performance audit period.

During our testing for the FISMA Core Metrics, OCIO did not provide requested documentation in a timely manner to demonstrate performance of its control activities for four of the nine applicable FISMA Metric Domains (RM, IAM, CM, and ISCM). Specifically, OCIO did not provide:

- Evidence related to system audit log reviews for two out of eight systems selected for testing.
- Supporting document relating to new privileged users' authorization access approvals for two out of eight systems selected for testing.
- Evidence demonstrating the effectiveness of controls associated with seven questions from the FY 2022 Core IG Metrics for one out of eight systems selected for testing.

We were informed by OCIO management that their inability to provide us with requested documentation was a result of competing priorities and lack of resources. However, we received enough supporting documentation for each of the impacted areas to assess the maturity levels of the applicable FY 2022 Core IG Metrics. Therefore, we were still able to assess the corresponding controls and determine the effectiveness of USDA's information security program.

Audit Recommendations and Findings

Finding 1: OCIO Needs to Comply with National Institute of Standards and Technology Special Publication 800-53, Revision 5

OCIO management has not implemented NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Federal Information System and Organization*, security control requirements for its information security program, as required by OMB Circular A-130, *Managing Information as a Strategic Resource*.

Specifically, OMB Circular A-130 requires agencies to apply NIST guidelines by updating associated processes and controls within 1 year of publication unless otherwise directed by OMB. For legacy information systems, agencies are expected to meet NIST standards and guidelines within 1 year of their respective publication dates unless otherwise directed by OMB. The 1-year compliance date for revisions to NIST publications applies only to new or updated material in the publications. For information systems under development, as well as legacy systems undergoing significant changes, agencies are expected to meet and follow the requirements of NIST standards and guidelines immediately upon deployment of the systems.

NIST SP 800-53, Rev. 5, was published on September 23, 2020; therefore, according to OMB Circular A-130, OCIO was required to fully comply within 1 year of publication (i.e., September 23, 2021). Due to OCIO management not having sufficient resources, OCIO was unable to update associated policies, procedures, processes, and controls to satisfy requirements to comply with NIST SP 800-53, Rev. 5, within the period mandated by OMB Circular A-130.

NIST SP 800-53, Rev. 5, includes new and updated security control requirements that offer a proactive and systematic approach to ensuring that critical systems, components, and services are sufficiently trustworthy and have the necessary resilience to defend against external attacks, misuse, and/or compromise. Without updating OCIO's security policies in accordance with NIST SP 800-53, Rev. 5, the likelihood is increased that OCIO is vulnerable to new and emerging threats, which can result in an increased risk to the confidentiality, integrity, and availability of OCIO information systems and data.

Recommendation 1 – Prioritize resources to implement NIST SP 800-53, Rev. 5, security control requirements for the OCIO information security program in accordance with OMB A-130.

Finding 2: OCIO Needs a Process to Formally Transition Authorizing Officials

The designated Authorizing Officials (AOs) changed for two of eight selected information systems; however, the new AOs did not approve a new authorization decision document for these systems. Specifically, our testing showed that for one information system the new delegated AO did not sign a new or updated authorization decision document, to formally transition the responsibility and accountability for affected systems and inherited controls. Similarly, for a second information system, the new delegated AO did not sign a new or updated authorization decision document.

OMB Circular A-130, *Managing Information as a strategic Resource*, states:

> "In the event that there is a change in AOs, the new AO reviews the current authorization decision document, authorization package, and any updated documents created as a result of the continuous monitoring activities. If the new AO is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls and explicitly accepting the risk. If the new AO is not willing to accept the previous authorization results (including the identified risk), a reauthorization action may need to be initiated or the new AO may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date."

OCIO management has not defined policies and procedures for formally transitioning responsibilities to a new AO. This includes those responsibilities related to the new AO's review of the current authorization decision documentation package and required documentation to justify their re-authorization decision for the information system. Our testing showed that, for one information system, the newly delegated AO did not sign a new or updated authorization decision document to formally transition the responsibility and accountability for affected systems and inherited controls. For a second information system, the newly delegated AO did not sign a new or updated re-authorization decision document.

Without the newly designated AO explicitly accepting the risk to organizational operations and assets, individuals, and other organizations, it may result in a lack of established responsibility and accountability for the information systems. This may lead to the AO not understanding and, as a result, not being responsive to the inherent and residual risks as well as the internal and external threats and vulnerabilities to the system.

Recommendation 2 – Document and implement a process for formally transferring responsibility when there is a change to the designated AO.

Recommendation 3 – Verify that all selected systems and inherited controls that transferred AOs and have not been re-authorized have formally transferred responsibility for the system or inherited controls.

Finding 3: OCIO Needs to Review Privileged User Accounts

OCIO management did not recertify access belonging to 1 of 25 privileged users selected for testing who had access to two of the eight selected information systems.

USDA Departmental Regulation (DR) 3505-003, *Access Controls for Information and Information Systems*, July 17, 2019, states:

> "Agencies will develop, implement, and maintain agency processes and procedures aligned with this DR to manage access to USDA information and information systems, ensuring the procedures: (1) Grant access only to individuals who have an established need-to-know

> and who meet the minimum interim or full background investigation requirements consistent with the system and level of access being requested; (2) Include monitoring and periodic validation of accounts and privileges. The frequency for audits will be as follows: privileged user accounts/groups each quarter (or a portion of the accounts/groups more frequently).

OCIO management informed us that they transitioned to a new identity management system in January 2022. During the transition, the account access of one selected privileged user was not successfully transferred to the new system; therefore, their privileged account access was not reviewed and recertified.

Lack of review and recertification of privileged users could lead to an increased risk of unauthorized access to and modification of production data and computing resources.

Recommendation 4 – Ensure that privileged user reviews are completed in accordance with DR 3505-003.

Recommendation 5 – Verify controls to ensure that all privileged users are successfully transferred to the identity management system.

Finding 4: OCIO Needs to Comply with Personal Identifiable Information Breach Requirements

OCIO management did not sufficiently implement a control to communicate a major incident involving the breach of Personal Identifiable Information (PII) information in a timely matter to stakeholders. On May 4, 2022, USDA National Finance Center (NFC) mailed 69,708 Federal Employee Calendar Year 2020 Corrected Wage and Tax Statements to the wrong address, resulting in a breach of sensitive PII. NFC was informed of this breach on May 19, 2022, but did not communicate the incident to the Agriculture Security Operations Division (ASOD) Cybersecurity Incident Response Team (CSIRT) until June 6, 2022.

USDA DR 3505-005, *Cybersecurity Incident Management*, November 30, 2018, states that all suspected or actual incidents should be reported to the ASOD CSIRT within 1 hour of discovery. Furthermore, DR 3505-005 requires heads of mission areas, agencies, and staff offices to perform the following:

> (1) Ensure that the provisions of this policy are implemented for the information resources that support the operations and assets under their control; and
>
> (2) Ensure that personnel in their area of responsibility perform their incident management responsibilities, including notification and reporting, in a timely manner and in accordance with Federal and Departmental requirements.

OCIO management informed us that, because of the lack of personnel knowledge and training, USDA NFC personnel were unable to identify and report the suspected PII breaches within the required timeframe defined by DR 3505-005. This information was later confirmed based on our

review of the documentation submitted in support of the incident closure package. Specifically, we reviewed email correspondence indicating NFC personnel was unsure of whether the incident should be classified as a PII breach, how this determination is made, and the overall USDA reporting procedures.

By not reporting suspected incidents involving PII in a timely manner, there is an increased risk that the PII of individuals was potentially compromised. Additionally, there is an increased risk that USDA is exposed to reputational scrutiny, costs impacting the agency budget (i.e., fines), and the potential of unlawful use of the compromised PII information.

Recommendation 6 – Provide targeted PII trainings to the impacted mission area in a more frequent manner to ensure mission area personnel are properly trained in identifying and reporting PII incidents and breaches in a timely manner.

Finding 5: OCIO Needs to Provide Sufficient Audit Evidence Timely

OCIO management did not retain evidence to demonstrate the effective implementation of control activities for RM, IAM, and ISCM, three Core FY 2022 Metric Domains. Specifically, for three systems selected, OCIO could not provide relevant documentation as required by the Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government (the "Green Book").* GAO's *Green Book* requires entities, such as USDA, to develop and maintain readily available documentation to evidence the implementation of their internal control systems.

Federal agencies, like USDA, are required to comply with GAO's *Green Book* and maintain readily available this information for auditor review. For two of the systems selected, OCIO could not provide support (i.e., audit log reviews and privileged users authorization access approvals) to document the controls were designed, implemented, and operating effectively. Additionally, for one system, we did not receive audit evidence.

GAO, *Standards for Internal Control in the Federal Government Documentation of the Internal Control System*, states:

> 3.09 - Management develops and maintains documentation of its internal control system.
>
> 3.10 - Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.
>
> 3.11 - Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

GAO, *Government Auditing Standards*, July 2018, section 1.03, states:

> As reflected in applicable laws, regulations, agreements, and standards, management and officials of government programs are responsible for providing reliable, useful, and timely information for transparency and accountability of these programs and their operations. Legislators, oversight bodies, those charged with governance, and the public need to know whether (1) management and officials manage government resources and use their authority properly and in compliance with laws and regulations; (2) government programs are achieving their objectives and desired outcomes; and (3) government services are provided effectively, efficiently, economically, and ethically.

Due to competing priorities, resource limitations, and scheduling constraints, OCIO management was unable to provide requested audit documentation within the designated period, which prevented us from testing core aspects of USDA's control environment. Without establishing internal controls that maintain readily available documentation evidencing the implementation and operation of a control, OCIO management cannot communicate the performance of those controls. Consequently, controls cannot be independently monitored and evaluated by OCIO management, auditors, and other stakeholders. In addition, ineffectively implemented controls for processes related to access authorizations and audit log reviews could lead to an increased risk of unauthorized access to and modification of an application's production data and computing resources.

Recommendation 7 – Design and implement a process to ensure risk management, identity and access management, and information security continuous monitoring internal control documentation is retained to support its system of internal controls and operational needs, as required by GAO's *Standards for Internal Control in the Federal Government Documentation of the Internal Control System*.

Conclusion

USDA's information security program was not effective for the five Cybersecurity Functions and nine FISMA Metric Domains as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. We identified findings in four of five Cybersecurity Functions and six of nine FISMA Metric Domains based on the procedures we performed related to the eight selected information systems reviewed, along with Department-wide testing procedures. Based on the CyberScope results, USDA's information security program was assessed as not effective because a majority of the FY 2022 IG FISMA Reporting Metrics were rated as Consistently Implemented (Level 3).

We issued five findings and made seven recommendations related to these findings that should strengthen USDA's information security program if effectively addressed by management. The root causes that led to the findings identified as part of this performance audit may contribute to findings for other systems outside of the scope of this audit.

For improving the maturity of the USDA information security program, USDA should consider applying these recommendations to its entire universe of systems. Further, USDA should implement robust monitoring capabilities to continually assess the security state of these systems to include a process to hold service centers accountable for identified compliance gaps.

In a written response, the CIO concurred with our findings and recommendations. (See Appendix IV: Agency's Response to Audit Report).

Appendix I: Glossary of Terms

AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ASOD	Agriculture Security Operations Division
CEC	Client Experience Center
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSIRT	Cybersecurity Incident Response Team
DHS	Department of Homeland Security
DISC	Digital Infrastructure Service Center
DPP	Data Protection and Privacy
DR	Departmental Regulation
EO	Executive Order
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAGAS	Generally Accepted Government Auditing Standard
GAO	Government Accountability Office
IAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISC	Information Security Center
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG, LLC
NFC	National Finance Center
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
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information
POA&M	Plan of Action and Milestone
RM	Risk Management
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event management
SOP	Standard Operating Procedure
SP	Special Publications
ST	Security Training
U.S.	United States
USDA/Department	United States Department of Agriculture

The subsequent sections of the report are not being publicly released due concerns about the risk of circumvention of law:

Appendix II—FY 2022 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (pages 14–33); and
Appendix III—Status of Prior Recommendations (pages 34–38).

Appendix IV: Agency's Response to Audit Report

United States Department of Agriculture

Office of the Secretary

Office of the Chief Information Officer

1400 Independence Avenue S.W. Washington, DC 20250

TO: Yarisis Rivera Rojas
Acting Assistant Inspector General for Audit
Office of Inspector General

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

GARY WASHINGTON

Digitally signed by GARY WASHINGTON
Date: 2022.09.20 10:27:17 -04'00'

SUBJECT: Office of Inspector General Audit #50503-0009-12, Fiscal Year 2022 "Federal Information Security Modernization Act"

The Office of the Chief Information Officer (OCIO) has reviewed the Office of the Inspector General's (OIG) draft report, "Federal Information Security Modernization Act Audit", Fiscal Year 2022 #50503-0009-12 and concurs with the findings and recommendations in the report.

OCIO will work with Mission Area Assistant Chief Information Officers (ACIOs) and key OCIO stakeholders to develop our Management Decision which will include our specific plan of action and milestones to assess, design, and implement solutions.

OCIO appreciates the work of the OIG in conducting its review and issuing this report. OCIO will utilize OIG's assessment to continue to strengthen management and technical controls over its Information Technology Security Program.

We look forward to receiving the final OIG report.

If additional information is needed, please contact Megen Davis, Director, Strategic Planning, E-Government and Audits, at (202) 631-1266 or via email at megen.davis@usda.gov.

cc: Ja'Nelle DeVore, CISO, OCIO
Terence Goodman, DCISO, OCIO
Maria Vlioras, Executive Assistant, CIO, OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Garcia Smith, Executive Assistant, DCISO, OCIO
Megen Davis, Director, Strategic Planning, E-Government and Audits, OCIO-IRMC
Mohammad Nikravesh, Audit Liaison Official, OCIO-IRMC
Alanna Watkins, Policy, and Compliance Branch Chief, OCIO-ISC
Cutina Mosley, IT Security Specialist, OCIO-ISC

Learn more about USDA OIG
Visit our website: **usdaoig.oversight.gov**
Follow us on Twitter: @OIGUSDA

How to Report Suspected Wrongdoing in USDA Programs

Fraud, Waste, and Abuse
File complaint online: **usdaoig.oversight.gov/hotline**

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)