U.S. Department of Agriculture
Office of Inspector General

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2025 Federal Information Security Modernization Act

July 2025

Audit Report 50503-0014-12

IMPORTANT NOTICE

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

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

Appendix II — FY 2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (pages 22–37); and
Appendix III— Status of Prior Recommendations (pages 38–44)

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2025 Federal Information Security Modernization Act

Audit Report 50503-0014-12

As required by FISMA, OIG reviewed USDA's ongoing efforts to improve its information technology security program and practices during FY 2025.

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. This included security controls at both the Department level and system level. Out of 212 information systems that support USDA missions, we selected [redacted] USDA-operated and [redacted] contractor-operated systems to perform system-level testing to determine whether the security controls were implemented and operated as intended.

RECOMMENDS

We made 11 recommendations related to these findings that, when implemented, should strengthen USDA's information security program if effectively addressed by management. To improve the maturity of its information security program, USDA should consider applying these recommendations to its entire universe of systems.

WHAT OIG FOUND

The U.S. Department of Agriculture (USDA) has worked diligently to improve its security posture, with the maturity level rising from the previous year. Consistent with the Federal Information Security Modernization Act (FISMA) requirements, the Office of Management and Budget (OMB) policy and guidance, and the National Institute of Standards and Technology standards and guidance, [redacted]

OMB establishes standards for an effective level of security and considers level 4, "Managed and Measurable," to be sufficient. We found USDA's maturity level is 4, which is effective according to OMB's criteria. However, weaknesses still exist, and we made 11 new recommendations to address 6 identified deficiencies within USDA's information security program. [redacted]

USDA OFFICE OF INSPECTOR GENERAL
United States Department of Agriculture

DATE: July 29, 2025

AUDIT NUMBER: 50503-0014-12

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

ATTN: Sherry Golden
Audit Liaison Official
IT Policy and Audits Division (IPAD)

FROM: Yarisis Rivera-Rojas
Assistant Inspector General for Audit

YARISIS RIVERA ROJAS
Digitally signed by YARISIS RIVERA ROJAS
Date: 2025.07.29 08:25:09 -04'00'

SUBJECT: U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2025 Federal Information Security Modernization Act

The Office of Inspector General contracted with KPMG LLP, an independent certified public accounting firm, to conduct an audit 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. This report presents the results of the subject review. The instructions for the fiscal year (FY) 2025 review are outlined in the Inspector General Federal Information Security Modernization Act of 2014 and Office of Management and Budget (OMB) Memorandum M-25-04 reporting guidance for FISMA, dated January 15, 2025. This report contains responses to the questions contained in these instructions. The contract required that the audit be performed in accordance with Government Auditing Standards and OMB guidance.

We found USDA's maturity level is 4, which is effective according to OMB's criteria. However, weaknesses still exist, and we made 11 new recommendations to address 6 identified deficiencies within USDA's information security program. **This report contains sensitive content. It is being withheld from public release due to concerns about the risk of circumvention of law.**

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2025 Federal Information Security Modernization Act

July 14, 2025

kpmg.com

KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

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

U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2025 Federal Information Security Modernization Act

This report presents the results of our independent performance audit of the United States (U.S.) Department of Agriculture's (USDA) information security program and practices for its information systems. We conducted our performance audit from November 5, 2024, through May 31, 2025, and our results are through the period of October 1, 2024, through June 30, 2025.

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 objectives of this performance audit were to:

1. Evaluate the effectiveness of the USDA's overall information technology (IT) security program by evaluating the six Cybersecurity Framework security functions outlined in the Office of Management and Budget's (OMB) Fiscal Year (FY) *2025 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2025 IG FISMA Metrics):
    - Govern, which includes questions pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
    - Identify, which includes questions pertaining to Risk and Asset Management;
    - Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
    - 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.

2. Follow up on the status of corrective actions taken by the Office of the Chief Information Officer (OCIO) to implement the Office of Inspector General's (OIG) prior performance audit recommendations and determine whether corrective actions for open FISMA recommendations are effectively implemented.[1]

As a result of our procedures and based on the maturity levels calculated using CyberScope, we assessed USDA's information security program as Managed and Measurable (Level 4), which was effective according to the FY 2025 IG FISMA Reporting Metric guidance. We made this determination based on assessing a majority of the IG Metrics as "Consistently Implemented" and "Managed and Measurable." Specifically, Govern and Recover cybersecurity functions were assessed as "Consistently Implemented." Further, the Identify, Protect, and Detect cybersecurity functions were assessed as "Managed and Measurable", and the Respond cybersecurity function was assessed as "Optimized" (see Appendix II).

We reported 6 new findings and made 11 recommendations related to these findings that, when implemented, should strengthen USDA's information security program if effectively addressed by management. We also evaluated the implementation of recommendations identified in the FY 2022, FY 2023, and FY 2024 FISMA performance audits. We determined that 14 of 28 recommendations remained open, and 14 recommendations were closed by management. The 14 recommendations that were closed were validated by us as effectively remediated and assigned a status of "Closed." (See Appendix III: Status of Prior Recommendations).

We caution that projecting the results of our performance audit 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, Department of Homeland Security (DHS), Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

July 14, 2025

[1] Audit Report 50503-0009-12, *Fiscal Year 2022 Federal Information Security Modernization Act*, Sept. 27, 2022; Audit Report 50503-0011-12, *Fiscal Year 2023 Federal Information Security Modernization Act*, July 28, 2023; and Audit Report 50503-0012-12, *Fiscal Year 2024 Federal Information Security Modernization Act*, July 25, 2024.

Table of Contents

Background

KPMG LLP (KPMG) performed the fiscal year (FY) 2025 independent Federal Information Security Modernization Act of 2014 (FISMA) audit, under contract with the United States Department of Agriculture (USDA) and on behalf of USDA Office of Inspector General (OIG), as a performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and the Consultant Standards established by the American Institute of Certified Public Accountants (AICPA). USDA OIG monitored our work to ensure that 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 USDA'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 USDA. 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 USDA's critical systems.

Agency Overview

USDA's mission is to provide leadership on food, agriculture, natural resources, rural development, nutrition, and related issues based on public policy, the best available science, and effective management.

Program Overview

USDA's Office of the Chief Information Officer (OCIO) operates as a Staff Office reporting to the Secretary and has a mission of serving the information needs for USDA. OCIO supports the achievements of USDA's 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 four service centers, all of which fall under the purview of OCIO: Cybersecurity & Privacy Operations Center (CPOC), Digital Infrastructure Services Center (DISC), Client Experience Center (CEC), and Information Resource Management Center.

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed FISMA[2] 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.

FY 2025 IG FISMA Reporting Metrics

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officers and Chief Information Security Officers councils, released OMB's guidance for implementing the requirements outlined in OMB Memorandum (M) 25-05, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, outlined in the *FY 2025 Inspector General FISMA Reporting Metrics* (IG Metrics). The FY 2025 IG Metrics are aligned with the six information security functions outlined in the *National Institute of Standards and Technology* (*NIST) Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework): Govern, Identify, Protect, Detect, Respond, and Recover. CIGIE maintained the maturity models for the following 10 FISMA Metric Domains: Cybersecurity Governance (CG), Cybersecurity Supply Chain Risk Management (C-SCRM), Risk and Asset Management (RAM), Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** illustrates the alignment of NIST Cybersecurity Framework to the FISMA Metric Domains within the FY 2025 IG FISMA Reporting Metrics. In Appendix VI, we discuss the significant changes to the IG Metrics from FY 2021 through FY 2025.

[2] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No.107-347, tit. III, Section 301, Subsection 3544(a)(1)(A), Dec. 17, 2002.

Table 1: Alignment of NIST Cybersecurity Framework to the FISMA Metric Domains

Cybersecurity Framework Functions	FISMA Metric Domains
Govern	Cybersecurity Governance Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Consistent with FY 2024, the model has five maturity levels: *Ad hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function.

Table 2: 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, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The FY 2025 IG FISMA Reporting Metrics included the removal of each Supplemental Metric from the FY 2023-FY 2024 IG FISMA Reporting Metrics. The Metrics still include both Core and Supplemental Metrics; however, the Supplemental Metrics were tailored to the Administration’s priorities. The FY 2025 IG FISMA Reporting Metrics included Core Metrics and Supplemental Metrics, as depicted in **Table 3.**

Table 3: FY 2025 Metric Scoping

Core Metrics	Supplemental Metrics
5 - SCRM Processes 7 - System Inventory 8 - Hardware Inventory 9 - Software Inventory 11 - Enterprise Risk Management & Risk Assessments 12 - Risk Management (RM) Dashboards and Reporting 14 - Configuration Settings 15 - Flaw Remediation 17 - Multi-factor Authentication (MFA) - General Users 18 - MFA - Privileged Users 19 - Privileged User Account Management 21 - Encryption 22 - Data Exfiltration and Network Defenses 24 - Workforce Assessment 26 - ISCM Strategy 28 - ISCM Processes 30 - Incident Response Tools and Detection 31 - Incident Response Tools and Handling 33 - Business Impact Analysis 34 - Information System Contingency Plan (ISCP) Test, Training, and Exercise	1 - Agency Cybersecurity Profiles 2 - Cybersecurity Risk Management Strategy 3 - Cybersecurity Roles and Responsibilities 15 - Data Inventory 27 - System Integrity and Security Posture Monitoring

IG FISMA Reporting Metrics Scoring

According to the FY 2025 IG FISMA Reporting Metrics guidance, a security program is considered effective if the calculated average of the Metrics in a particular Domain is Managed and Measurable (Level 4) or higher. For FY 2025, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics were averaged independently to determine a Domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core Metrics and Supplemental Metrics were used as a data point to support the risk-based determination of overall program and function level effectiveness. Other data points considered included:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the review period;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Reported security incidents reported during the review period.

IGs should use the CyberScope[3] reporting tool to calculate the maturity levels for each Cybersecurity Function and Domain and to submit the results of the IG Metrics evaluation. CyberScope provides supplementary fields to allow explanatory comments; IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and ultimately provide the overall effectiveness of the USDA's information security program.

[3] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, Offices of Inspectors General provide an independent assessment of effectiveness of an agency's information security program. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

Objective, Scope, and Methodology

Objective

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objectives of this performance audit were to:

1. Evaluate the effectiveness of USDA's overall IT security program by evaluating the six Cybersecurity Framework security functions outlined in the FY 2025 IG FISMA Metrics:

    - Govern, which includes questions pertaining to Cybersecurity Governance and Cybersecurity Supply Chain Risk Management;
    - Identify, which includes questions pertaining to Risk and Asset Management;
    - Protect, which includes questions pertaining to Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training;
    - 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.

2. Follow up on the status of corrective actions taken by the OCIO to implement OIG's prior performance audit recommendations and determine whether corrective actions for open FISMA recommendations are effectively implemented for the corresponding FY 2025 IG Metric questions.[4]

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2025 IG Metrics; applicable NIST standards and guidelines, presidential directives, OMB memorandums referenced in the reporting metrics; and USDA policies and procedures. We performed procedures to assess whether selected controls established by USDA's information security program were designed, implemented, and operating effectively from both an entity-wide and system-level perspective.

We performed testing at the entity level, which included OCIO and the following service centers that were significant to this performance audit:

- CPOC serves and supports USDA Agencies and Offices by helping to protect their mission-critical assets and information, thereby securing the country's food, agriculture, rural, and natural resources programs.

- DISC is responsible for the management and operation of the Data Center Hosting Services including the USDA Enterprise Data Centers in Kansas City, Missouri and Chicago, Illinois.

[4] *Supra* note 1.

- CEC is a Federal Government information-technology service provider that uses a business model to support the comprehensive IT requirements of Federal business. CEC provides comprehensive information technology, associated operations, security, and technical-support services to USDA field, State, and headquarters offices across the U.S. and its territories, which include: Puerto Rico, Guam, U.S. Virgin Islands, Northern Mariana Islands, and Pacific Basin.[5]

We also selected [redacted] USDA-operated and [redacted] contractor-operated information systems out of 212 information systems that support USDA missions to perform system-level testing to determine whether the security controls were suitably designed, implemented, and operating effectively.

USDA's responsibilities as it relates to USDA-operated and contractor-operated systems differ. USDA's primary responsibilities with respect to contractor-operated systems are to monitor the effective information system controls of the systems and to help ensure the risk related to these systems did not exceed USDA's risk tolerance. Accordingly, the contractor-operated systems were subjected to a different set of performance audit procedures from the USDA-operated information 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 objective.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the 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 non-statistical random selections where the sizes of the populations (i.e., the number of occurrences of the control) were the 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:

[5] www.usda.gov/ocio/centers.

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
Recurring Manual (multiple times/day) (>5000) [6]	45

The following approach was agreed upon with USDA OIG for conducting this performance audit and determining the maturity levels for each of the 6 Cybersecurity Functions and 10 FISMA Metric Domains from the Core Metrics and Supplemental Metrics:

- We requested OCIO 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 security controls referenced in FY 2025 IG Metrics that system support teams performed to secure USDA information systems (where applicable), leveraging maturity Level 3 (Consistently Implemented) capabilities within the 10 FY 2025 IG FISMA Reporting 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) capabilities within the 10 IG FISMA Reporting Metric Domains. If we identified findings associated with Metrics that were tested in consideration of maturity Level 4, 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) capabilities within the 10 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

[6] In accordance with the Government Accountability Office *Financial Audit Manual*, Volume 1, June 2025, GAO-25-107705.

Level 5, we assessed the maturity at Level 4 for the questions with responses indicating control failures.

Per the results of our test procedures, we entered the assessed maturity level for each of the Core Metrics and Supplemental Metrics into the CyberScope[3] reporting tool, which automatically calculated the average core and supplemental ratings for Domains and Functions.

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 Department, Mission Area, and system levels.

We performed our fieldwork from November 5, 2024, through May 31, 2025. Our testing was performed remotely through meetings, walkthroughs, and observations with representatives from USDA. During our performance audit, we met with OCIO and the Mission Areas to discuss our findings and recommendations.

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. We also leveraged a variety of USDA directives, manuals, standard operating procedures, and other system-level guidance for information security.[7] For each finding detailed in the Audit Findings and Recommendations section, we included the relevant USDA, OMB, and/or NIST criteria.

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

Overall Results

[redacted]

[redacted]

As a result, we assessed USDA's information security program as Managed and Measurable (Level 4), which was effective according to OMB's FY 2025 IG Metrics guidance. **Table 5** below depicts USDA's maturity levels for the six Cybersecurity Functions.

Table 5: Maturity Levels for Cybersecurity Functions

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
1. Govern Cyber Governance (CG) Cybersecurity-Supply Chain Risk Management (C-SCRM)	*1. Govern: Level 3: Consistently Implemented* CG – Level 4: Managed and Measurable C-SCRM – Level 3: Consistently Implemented
2. Identify Risk and Asset Management (RAM)	*2. Identify: Level 4: Managed and Measurable* RAM – Level 4: Managed and Measurable
3. Protect Configuration Management (CM) Identity Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)	*3. Protect: Level 4: Managed and Measurable* CM – Level 2: Defined IAM – Level 4: Managed and Measurable DPP – Level 4: Managed and Measurable

[8] *Supra* note 1.

[9] Recommendations 7 and 8 were reissued from prior year audits.

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
	ST – Level 4: Managed and Measurable
4. Detect Information Security Continuous Monitoring (ISCM)	*4. Detect: Level 4: Managed and Measurable* ISCM – Level 4: Managed and Measurable
5. Respond Incident Response (IR)	*5. Respond: Level 5: Optimized* IR – Level 5: Optimized
6. Recover Contingency Planning (CP)	*6. Recover: Level 3: Consistently Implemented* CP – Level 3: Consistently Implemented
Overall Maturity Level	**Level 4: Managed and Measurable**
Overall Effectiveness	**Effective**

Source: CyberScope Appendix A: Scoring Maturity Model.

Audit Recommendations and Findings

The following sections provide a summary of the audit recommendations and findings for each of the FISMA Metric Domains required to be monitored under FISMA. We did not identify any new findings or recommendations for the CG, C-SCRM, DPP, ST, ISCM, IR, and CP FISMA Metric Domains and have, therefore, omitted them from this section.

Risk and Asset Management

The FY 2025 IG Metrics state that the Risk and Asset Management (RAM) Domain focuses on policies and actions that effectively manage information security risks within the organization. Federal agencies are required to consistently implement their security architecture across the enterprise, business process, and systems. The performance audit determined that USDA's risk management maturity level was Managed and Measurable (Level 4). To improve security in this Domain, USDA should address the following issues:

Finding 1 [redacted]

[redacted]

[redacted][10]

[redacted][10]

[redacted][11] [redacted]

[10] [redacted]

[11] Federal Information Processing Standards-199 establishes security categories for Federal information systems based on the potential impact on an organization if certain events compromise the information or systems. The security categories are determined by evaluating the impact on three security objectives: confidentiality, integrity, and availability. These categories are defined as Low, Moderate, and High. A rating of high indicates that the loss of confidentiality, integrity, and availability could have severe or catastrophic adverse effect on organizational operations, assets, or individuals. A high impact level might result in a major financial loss, significant harm to individuals, or severe impact on organizational effectiveness.

[redacted]

Recommendation 1 *–* [redacted]

Recommendation 2 *–* [redacted]

Recommendation 3 *–* [redacted]

Finding 2 [redacted]

[redacted]

[redacted]

[redacted][12]

[redacted]

[12] The Federal Financial Management Improvement Act of 1996 aims to enhance Federal financial management by ensuring that Federal financial management systems provide accurate, reliable, and timely financial information to Government managers. It requires Federal agencies to implement and maintain financial management systems that comply with Federal requirements, accounting standards, and the U.S. Government Standard General Ledger.

[redacted][13]

[redacted]

[redacted]

Recommendation 4 – [redacted]

Recommendation 5 – [redacted]

Recommendation 6 - [redacted]

Finding 3 [redacted]

[redacted]

[redacted][15]

[redacted]

[13] Office of Management and Budget (OMB) Memorandum 23-06, Appendix D, Management of Financial Management Systems – Risk and Compliance, December 23, 2022.

[14] USDA Standard Operating Procedures for Risk Management Framework, Step 1: Categorize Information Systems, Version 1.1, May 2022, SOP-3440-003E.

[15] USDA Standard Operating Procedures for Interconnection Security Agreements, CPOC Security Management Division (SMD), Version 4, June 22, 2022, SOP-3540-003D.

[redacted]

[redacted][16]

Recommendation 7 - [redacted]

Recommendation 8 - [redacted]

Configuration Management

The CM Domain focuses on policies and actions that effectively manage how agencies develop an information security program to enable compliance with minimally acceptable system configuration requirements. CM refers to a collection of control activities focused on establishing and maintaining the integrity of products and information systems through processes for initializing, changing, and monitoring their configurations.

Finding 4 [redacted]

[redacted]

[redacted]

[redacted]

[16] Audit Report 50503-0012-12, *Fiscal Year 2024 Federal Information Security Modernization Act*, July 25, 2024 (FY24 Rec 1 and FY24 Rec 2, see Appendix III).

[17] Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities, July 14, 2022.

Table 6: USDA Late Vulnerability Remediation[18]

Days Outstanding Past Due Date	1 to 30 Days	31 to 60 Days	61 to 90 Days	Over 90 Days
Critical Vulnerabilities	[redacted]	[redacted]	[redacted]	[redacted]
High Vulnerabilities	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted][20]

[redacted]

[redacted][21]

[18] [redacted]
[19] USDA Departmental Regulation (DR) 3565-003, Plan of Action and Milestones Policy, September 25, 2013.
[20] USDA DR 3530-006, Scanning and Remediation of Configuration and Patch Vulnerabilities, June 5, 2019. DR 3530-006 has an expiration date of June 5, 2024, however USDA DR's are still valid until it is superseded or rescinded.
[21] [redacted]

Finding 5 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 9 – [redacted]

Identity and Access Management

The FY 2025 IG Metrics guidance states that the IAM Domain focuses on policies and actions that effectively manage how an agency must implement a set of capabilities to help ensure users authenticate IT resources and only have access to resources that are required for their job function—a concept referred to as “need to know.” The supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges. These activities collectively are referred to as Identity, Credential, and Access Management.

Finding 6 [redacted]

[redacted]

[redacted]

[redacted][2]

[redacted]

Recommendation 10 – [redacted]

Recommendation 11 – [redacted]

Conclusion

[redacted]

[redacted]

[22] As required by the selected system's SSP.

We assessed USDA’s information security program as Managed and Measurable (Level 4), which was effective according to OMB’s FY 2025 IG FISMA Reporting Metrics guidance.

In a written response, the Chief Information Officer generally concurs 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
CEC	Client Experience Center
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CG	Cyber Governance
CM	Configuration Management
CP	Contingency Planning
CPOC	Cybersecurity & Privacy Operations Center
C-SCRM	Cybersecurity Supply Chain Risk Management
Cybersecurity Framework	National Institute Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
[redacted]	[redacted]
DHS	Department of Homeland Security
DISC	Digital Infrastructure Services Center
DPP	Data Protection and Privacy
DR	Departmental Regulation
FISMA	Federal Information Security Modernization Act of 2014
[redacted]	[redacted]
FY	fiscal year
FY 2025 IG FISMA Metrics	Fiscal Year 2025 Inspector General Information Security Modernization Act of 2014 Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
IAM	Identity and Access Management
IR	Incident Response
ISA	Interconnection Security Agreement
ISCM	Information Security Continuous Monitoring
IT	information technology
KPMG	KPMG LLP
[redacted]	[redacted]
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
[redacted]	[redacted]
OCIO	Office of the Chief Information Officer
[redacted]	[redacted]
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RAM	Risk and Asset Management
RM	Risk Management
[redacted]	[redacted]
SCRM	Supply Chain Risk Management
SP	Special Publications
SSP	System Security and Privacy Plan

ST	Security Training
U.S.	United States
USDA	U.S. Department of Agriculture

[redacted]

Inspector General

Section Report

2025

FISMA Annual IG

Department of Agriculture

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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: Janet Sorensen
Assistant Inspector General for Audit
Office of Inspector General

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

SUBJECT: Office of Inspector General Audit, *Fiscal Year 2025 Federal Information Security Modernization Act* #50503-0014-12

The Office of the Chief Information Officer (OCIO) has reviewed the Office of the Inspector General (OIG) audit report, *Fiscal Year 2025 Federal Information Security Modernization Act* #50503-0014-12 and generally 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.

The OCIO appreciates the work of the OIG in conducting its review and issuing this report. OCIO will utilize OIG's assessment to continue to mature its Information Technology Security program.

If additional information is needed, please contact Renae Harris-Hill, Director, IT Policy and Audits, at (202) 993-6071 or via email at maryrenae.harris-hill@usda.gov.

cc: Anthony Brannum, CISO, OCIO
Barry Lipscombe, DCISO, OCIO
Maria Vlioras, Executive Assistant, CIO, OCIO
Brittany Smith, Executive Assistant, CISO, OCIO
Renae Harris-Hill, Director, IT Policy and Audits, OCIO-IRMC
Sherry Golden, Audit Liaison Official, OCIO-IRMC

Sheryl Quinter, Director, Security Management Division, OCIO-CPOC
Alanna Watkins, Chief, Compliance Branch, OCIO-CPOC
Cutina Mosley, IT Security Specialist, OCIO-CPOC

Appendix V: IG FISMA Metric Change Over Time

Due to the significant changes to the IG FISMA Reporting Metrics (IG Metrics) year over year,

[redacted]

[redacted]

[redacted]

[redacted]

Learn more about USDA OIG
at https://usdaoig.oversight.gov
Find us on LinkedIn: US Department of
Agriculture OIG
Find us on X: @OIGUSDA

Report suspected wrongdoing in USDA programs:

https://usdaoig.oversight.gov/hotline-information

U.S. Department of Agriculture (USDA) is an equal opportunity provider, employer, and lender.

All photographs on the front and back covers are from USDA Flickr and are in the public domain. They do not depict any particular audit, inspection, or investigation.