U.S. Department of Agriculture
Office of Inspector General

Administration of USDA's Information Technology Regulations and Policies

March 2026

Inspection Report 50801-0016-12








Administration of USDA's Information Technology Regulations and Policies

Inspection Report 50801-0016-12

We determined that USDA's IT security directives are not sufficiently relevant and effective to address recent threats, as they are not consistently updated and some are similar in content or function, resulting in potential risks to USDA's IT security posture.

OBJECTIVE

Our objective was to determine whether USDA's information technology regulations and policies were sufficiently relevant and effective to address information technology security threats.

BACKGROUND

OCIO provides oversight and support for USDA's IT and cybersecurity activities. This inspection was partly initiated in response to findings from the Office of Inspector General's prior audit report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2021 Federal Information Security Modernization Act* (50503-0005-12). Specifically, auditors identified issues with USDA's IT security regulations and policies and the timeliness of OCIO's policy reviews. Although the recommendations were closed as of August 1, 2022, our review found that issues remain.

REVIEWED

Our scope covered USDA's IT regulations and policies, applicable to all mission areas and staff offices, within the Information Resources Management directive category, in effect as of January 2025.

WHAT OIG FOUND

We found that 10 of the 32 U.S. Department of Agriculture (USDA) information technology (IT) security directives we reviewed were not updated to reflect recent changes in threats, technology, and cybersecurity requirements. For example, the directives were not updated to ensure compliance with Security and Privacy Controls for Information Systems and Organizations, and did not align with recently issued cybersecurity directives on encryption. This occurred because the Office of the Chief Information Officer (OCIO) does not have a formal, documented process, consistent with National Institute of Standards and Technology (NIST) to ensure that its cybersecurity directives are updated in response to emerging cybersecurity risks and evolving Federal guidance. Additionally, USDA maintains multiple cybersecurity directives that are similar in content or function which poses a risk of conflicting guidance, inconsistent implementation, and increased administrative burden. These risks may contribute to noncompliance of requirements and negatively impact public trust in the Department's IT security posture.

WHAT OIG RECOMMENDS

We recommend that OCIO: (1) document and implement a process to ensure emerging cybersecurity risks and potential compliance gaps are addressed timely in accordance with NIST guidance; and (2) implement a process to screen for duplication and overlap across Departmental directives during the drafting, review, and revision of IT security directives.

OCIO agreed with our findings and recommendations. We accepted management decision for the two recommendations.

USDA OFFICE OF INSPECTOR GENERAL
United States Department of Agriculture

DATE: March 23, 2026

INSPECTION NUMBER: 50801-0016-12

TO: Kimberly R. Jackson
Deputy Chief Information Officer
Office of the Chief Information Officer (OCIO)

ATTN: Sherry Golden
Audit Liaison Official
OCIO

FROM: Tiffany Hooper, Acting Deputy Assistant Inspector General for Audit
for Yarisis Rivera-Rojas, Acting Assistant Inspector General for Audit

SUBJECT: Administration of USDA's Information Technology Regulations and Policies

This report presents the results of our inspection of the Administration of USDA's Information Technology Regulations and Policies. Your written response to the official draft is included in its entirety at the end of the report. Based on your written response, we are accepting management decision for the two recommendations in the report, and no further response to this office is necessary.

In accordance with Departmental Regulation 1720-1, final action needs to be taken within 1 year of the date of each management decision. Please follow your internal agency procedures in forwarding final action correspondence to the Office of the Chief Financial Officer.

We appreciate the courtesies and cooperation extended to us by members of your staff during our fieldwork and subsequent discussions. This report contains publicly available information and will be posted in its entirety to our website (https://usdaoig.oversight.gov) in the near future.

Table of Contents

Background and Objective

Background

The Office of the Chief Information Officer (OCIO) provides oversight, leadership, and support for the Department's information technology (IT) applications, information management, technology investments, and cybersecurity activities in support of the U.S. Department of Agriculture (USDA) IT program delivery for individual USDA Mission Areas and Offices. Specifically, OCIO governs and provides policy oversight, including 214 total IT investments within USDA's $3.1 billion IT portfolio. USDA maintains IT regulations, policies, and other relevant guidance in its Directive library within the Information Resources Management category.

Federal agencies depend on IT systems to carry out operations and process, maintain, and report essential information.[1] The security of these systems and data is vital to protecting individual privacy and national security. Risks to technology systems are increasing, including cyberattacks that could result in serious harm to human safety, the environment, and the economy.

According to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, policy for managing cybersecurity risks should be reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.[2] Actions to implement this standard include updating policy based on periodic reviews of cybersecurity risk management results to ensure that policy:

- Incorporates risk adequately.
- Provides a timeline for reviewing changes to the organization's environment.
- Communicates recommended updates.
- Reflects changes in technology, business, and legal or regulatory requirements.

In audit report, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2021 Federal Information Security Modernization Act* (50503-0005-12), auditors found that IT security policies were not retired or superseded in a timely manner, and the Department's IT security policies and procedures were not revised when Federal requirements were changed. This increased the risk that security practices are outdated, unclear, misunderstood, or improperly implemented.[3]

The Federal Information Security Modernization Act (FISMA) audit team recommended that the Department retire or supersede IT security policies and procedures on the Department Directives website in a timely manner and use various communication methods during the policy clearance process to inform employees, contractors, and other stakeholders of required practices and

[1] Government Accountability Office (GAO), *High- Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (Apr. 2023).
[2] NIST, *Cybersecurity Framework 2.0* (Feb. 26, 2024).
[3] Audit Report 50503-0005-12, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2021 Federal Information Security Modernization Act*, Oct. 2021.

procedures. They also recommended updating IT security policies and procedures on its Directives website to include the most current Federal guidance. OCIO stated it would address these recommendations by (1) revising language to address future revisions of authoritative references; (2) issuing a Departmental Notice to implement the requirements and authoritative references; (3) providing an example of a recently updated directive; (4) providing governance documentation for directive reassignment or retirement plan; and (5) developing a plan to reassign, retire, or update aged IT security policies/procedures. Although the corrective actions for all recommendations were completed as of August 1, 2022, our review found that similar issues remain.

Objective

Our objective was to determine whether USDA's information technology regulations and policies were sufficiently relevant and effective to address information technology security threats.

Finding 1: USDA Cybersecurity Policy Management is Not Aligned With Federal Requirements

We found that 10 of the 32[4] USDA IT security directives we reviewed were not updated to reflect recent changes in threats, technology, and cybersecurity requirements.[5] This occurred because OCIO's policy does not have a formal, documented process, consistent with NIST, to ensure that cybersecurity directives are systematically reviewed and updated in response to emerging cybersecurity risks, evolving Federal guidance, and changes in cybersecurity expectations. As a result, USDA may delay implementation of key cybersecurity practices, overlook modern risks, and increase the agency's exposure to emerging technology vulnerabilities.

NIST suggests that policy for managing cybersecurity risks should be reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.[6] NIST also emphasizes the importance of receiving cyber threat intelligence; identifying and recording threats; and selecting, prioritizing, tracking, and communicating risk responses.[7]

We determined that USDA lacks a structured process to ensure its cybersecurity policies are reviewed and updated in response to evolving threats and Federal cybersecurity requirements, and that USDA's Cybersecurity Policy management is not aligned with Federal requirements (NIST). Specifically, we found 10 security directives that failed to address changes[8] in threats, technology, and cybersecurity requirements (see Figure 1).

[4] See Exhibit A for the list of the 32 USDA IT security directives we reviewed.
[5] As of September, 2025.
[6] NIST, *Cybersecurity Framework 2.0* (Feb. 26, 2024).
[7] Ibid.
[8] Changes refers to major cybersecurity directives published within the last 5 years.

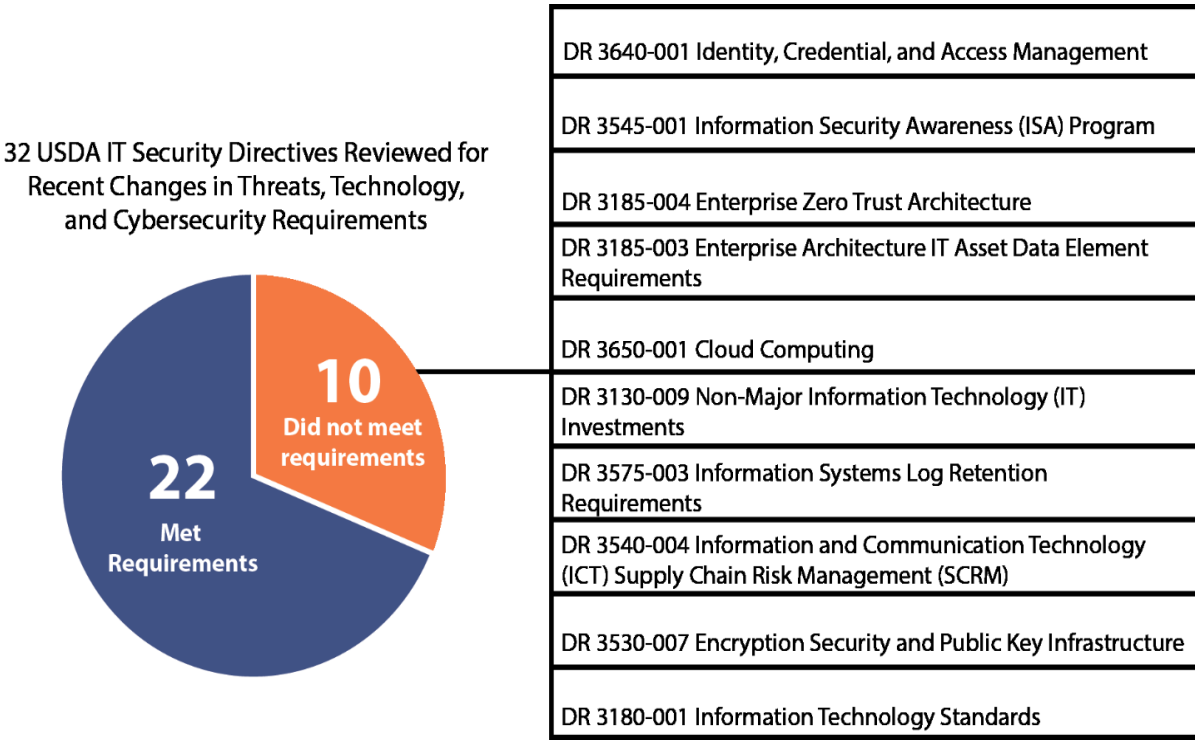

Figure 1: Chart showing 10 of the 32 USDA IT security directives, Departmental Regulations (DRs), we reviewed that did not address recent changes in threats, technology, and cybersecurity requirements. The remaining 22 directives met requirements. All directives reviewed are listed in Exhibit A. Figure by the Office of Inspector General (OIG).

Examples of potential threats not covered in the directives include: (1) compliance with guidance on *Security and Privacy Controls for Information Systems and Organizations*,[9] (2) alignment with recently issued cybersecurity directives on encryption, and (3) compliance with the latest guidance on supply chain security.

Although USDA requires an annual review of directives,[10] OCIO does not have a formal, documented process to ensure that changes in cybersecurity related requirements, threats, technology and organizational mission are captured timely and updated in its directives, consistent with NIST.[11] OCIO stated that directive updates are identified through annual gap analysis but have not been documented as a formal process due to staff capacity and workload, competing priorities, time constraints, and stakeholder availability.

Failing to update cybersecurity policies can expose USDA to risks, including operational inefficiencies and increased security vulnerabilities. Additionally, outdated policies may not align with current laws and regulations, leading to noncompliance with laws and regulations, data breaches, and reputational damage. Furthermore, outdated procedures can create inefficiencies, reduced productivity, and increased operational costs.

[9] NIST Special Publication 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (Sept. 2020).
[10] USDA DR-0100-001, *Departmental Directives System* (Jan. 4, 2018).
[11] NIST, *Cybersecurity Framework 2.0* (Feb. 26, 2024).

OCIO officials stated they are currently evaluating an automated process to help manage their IT policies; however, OCIO did not have an estimated date for when this automated process would be implemented.

Recommendation 1

Document and implement a process to identify, prioritize, track and communicate changes in cybersecurity requirements, threats, technology, and organizational mission as they occur to facilitate the review of directives at least annually to ensure emerging cybersecurity risks and potential compliance gaps are addressed timely.

Agency Response

OCIO agreed with this recommendation.

In its February 27, 2026, response, OCIO stated that it will document and implement a Standard Operating Procedure (SOP) to ensure that directives related to cybersecurity requirements, threats, technology and organizational mission are reviewed at least annually to address emerging risks and compliance gaps promptly.

OCIO provided an estimated completion date of September 30, 2026.

OIG Position

We accept management decision for this recommendation. For Final Action, provide the Office of the Chief Financial Officer (OCFO) with the SOP that ensures that directives related to cybersecurity requirements, threats, technology and organizational mission are reviewed at least annually to address emerging risks and compliance gaps promptly, along with evidence of its distribution. The SOP should highlight how OCIO will identify, prioritize, track and communicate changes in cybersecurity requirements as they occur, as well as outline the directive review process and timeline.

Finding 2: USDA Cybersecurity Policy Environment Includes Duplicative or Overlapping Directives

We found that USDA maintains multiple cybersecurity directives that are similar in content or function. Specifically, we found that 10 of the 32 USDA IT directives we reviewed had related subject matter, creating overlap. For example, we found four directives addressing IT Governance with duplicative guidance. This occurred because OCIO's policy does not explicitly include screening for duplication or overlap and did not identify any specific barriers preventing adoption of a more formal process, aside from noting the existence of informal controls.[12] As a result, the effectiveness of internal control activities are reduced, as duplicative policies could confuse users, leading to gaps in agency governance, risk management, and compliance.

According to GAO, management should implement control activities through policies and periodically review policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. This emphasizes that well-designed policies are foundational to internal control, and duplication undermines clarity, consistency, and effectiveness.[13]

We found that 10 of the 32 USDA IT security directives we reviewed had related subject matter, creating overlap. See Figure 2.

Figure 2: List of similar policies. Figure by OIG.

For example, the Enterprise Architecture Program directives (DR 3185-001 through DR 3185-003), contain interrelated and partially redundant content. However, OCIO had not identified the redundancy during its limited review. OCIO officials stated they do not have a formal automated process but instead conduct manual duplication checks during the policy review process and use internal tools—such as policy tracking and gap analysis reviews—to identify potential

[12] USDA Departmental Manual (DM) 0100-001, *Preparing Departmental Directives* (Jan. 4, 2018).
[13] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, ¶ 12.05 (Sept. 2014).

duplication or conflicting language across documents. Although these ad hoc controls may help reduce some overlap, we found that these controls are not fully effective, and improvements are needed.

According to NIST, organizations strengthen their cybersecurity risk governance practices by implementing repeatable, formally approved practices rather than relying on ad hoc approaches.[14] The absence of an effective, defined, and repeatable process limits the Department's ability to systematically prevent or address directive duplication. Such overlapping and duplicative IT security directives poses a risk of conflicting or inconsistent implementation, increased administrative burden for staff, and potential noncompliance with internal control requirements.

OCIO officials stated they are currently evaluating an automated process to help manage their IT policies; however, OCIO did not have an estimated date for when this automated process would be implemented.

Recommendation 2

Implement a process to screen for duplication and overlap across Departmental directives during the drafting, review, and revision of IT security directives.

Agency Response

OCIO agreed with this recommendation.

In its February 27, 2026, response, OCIO stated that it will document and implement a Standard Operating Procedure (SOP) to ensure that IT security directives are reviewed for duplication and overlap during the drafting, reviewing and revision processes.

OCIO provided an estimated completion date of September 30, 2026.

OIG Response

We accept management decision for this recommendation. For Final Action, provide OCFO with the SOP developed to screen for duplication and overlap and evidence of its distribution.

[14] NIST, *Cybersecurity Framework 2.0* (Feb. 26, 2024).

Scope and Methodology

We conducted our inspection to determine whether USDA's IT regulations and policies are sufficiently relevant and effective to address IT security threats. The scope of our inspection covered all 32 of USDA's IT regulations and policies within the Information Resources Management directive category that were in effect at the start of our inspection, January 2025. We conducted our fieldwork remotely between January 2025 and February 2026. We discussed the results of our inspection with agency officials on February 23, 2026, and included their comments, as appropriate.

To accomplish our objective, we:

- reviewed a relevant prior OIG audit,[15] which included recommendations to:
  - Retire or supersede IT security policies timely;
  - Update IT with current Federal guidance;
- interviewed OCIO officials, as necessary;
- obtained and reviewed other relevant documentation provided by the Department; and
- reviewed standards and policies related to the sufficiency of IT security regulations and policies to address current information security threats.

We did not independently review or assess the agency's information system(s); therefore, we make no representation regarding the adequacy of the agency's computer system(s), or the information generated from it. We specifically followed-up on the FISMA recommendations to confirm that the corrective actions for the recommendations were completed.

This inspection was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

[15] Audit Report 50503-0005-12, *U.S. Department of Agriculture, Office of the Chief Information Officer, Fiscal Year 2021 Federal Information Security Modernization Act,* Oct 2021.

Abbreviations

DM	Departmental Manual
DR	Departmental Regulation
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IT	information technology
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
SOP	Standard Operating Procedure
USDA	U.S. Department of Agriculture

Exhibit A: List of USDA IT Security Directives Reviewed

Count	Directive Number	Directive Name
1	DR 3105-001	USDA Chief Information Officers Council
2	DR 3111-001	USDA Information Technology Strategic Plan Process
3	DR 3130-008	Definition of Major Information Technology Investments
4	DR 3130-009	Non-Major Information Technology Investments
5	DR 3130-010	USDA Enterprise Information Technology Governance
6	DR 3130-013	Information Technology Capital Planning and Investment Control
7	DR 3145-001	Oversight and Management of the Federal Information Technology Acquisition Reform Act
8	DR 3170-001	End User Workstation Configurations
9	DR 3180-001	Information Technology Standards
10	DR 3185-001	Enterprise Architecture
11	DR 3185-002	Enterprise Architecture IT Asset Definitions
12	DR 3185-003	Enterprise Architecture IT Asset Data Element Requirements
13	DR 3185-004	Enterprise Zero Trust Architecture
14	DR 3300-001-A	Procuring and Managing Telecommunications Devices and Services
15	DR 3300-001-B	Telephone Use
16	DR 3300-001-E	Video Teleconferencing Facilities and Systems
17	DM 3410-001	Information Collection Procedures
18	DR 3410-001	Information Collection Activities - Collection of Information from the Public
19	DR 3450-001	Computer Matching Program Involving Personally Identifiable Information
20	DR 3460-001	Digital Signage Policy and Procedures within USDA Headquarters Facilities
21	DM 3465-001	Geospatial Metadata Standards
22	DR 3465-001	Enterprise Geospatial Data Management
23	DR 3515-002	Privacy Policy and Compliance for Personally Identifiable Information
24	DR 3530-007	Encryption Security and Public Key Infrastructure
25	DR 3540-004	Information and Communication Technology Supply Chain Risk Management
26	DR 3545-001	Information Security Awareness Program
27	DR 3575-003	Information Systems Log Retention Requirements
28	DR 3575-004	Information Technology Security Baselines and Security Control Tailoring
29	DR 3600-002	Electronic-Government Program
30	DR 3600-003	Robotic Process Automation Policy
31	DR 3640-001	Identity, Credential, and Access Management
32	DR 3650-001	Cloud Computing

Office of the Chief Information Officer's Response to Inspection Report

United States Department of Agriculture

DATE: February 27, 2026

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

FROM: Kimberly R. Jackson /s/
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Response to Recommendations in OIG Engagement No. 50801-0016-12

The Office of the Chief Information Officer (OCIO) submits the following response to the recommendations in the Office of Inspector General's (OIG) engagement 50801-0016-12 Administration of USDA's Information Technology Regulations and Policies.

Recommendation 1: Document and implement a process to identify, prioritize, track and communicate changes in cybersecurity requirements, threats, technology, and organizational mission as they occur to facilitate the review of directives at least annually to ensure emerging cybersecurity risks and potential compliance gaps are addressed timely.

Agency Response:

Agree with recommendation: X Yes __ No
Agree with monetary results: __ Yes __ No X N/A

In response to this recommendation, OCIO will document and implement a Standard Operating Procedure (SOP) to ensure that directives related to cybersecurity requirements, threats, technology and organizational mission are reviewed at least annually to address emerging risks and compliance gaps promptly.

OCIO will provide the following documentation:

- OCIO Directive SOP
- Evidence of distribution to OCIO center personnel with Directive responsibilities

Completion or Estimated Completion Date: **September *30, 2026***

Recommendation 2: Implement a process to screen for duplication and overlap across Departmental directives during the drafting, review, and revision of IT security directives.

Agency Response:

Agree with recommendation: X Yes __ No
Agree with monetary results: __ Yes __ No X N/A

In response to this recommendation, OCIO will document and implement a Standard Operating Procedure (SOP) to ensure that IT security directives are reviewed for duplication and overlap during the drafting, reviewing and revision processes.

OCIO will provide the following documentation:

- OCIO Directive SOP
- Evidence of distribution to OCIO center personnel with Directive responsibilities.

Completion or Estimated Completion Date: **September *30, 2026***

If additional information is needed, please contact Eric Shenton, Deputy Associate Chief Information Officer, at (202) 430-3791 or via email at eric.shenton@usda.gov.

cc: Samuel Berry, CIO
Denessa Moses, ACIO, OCIO-IRMC
Eric Shenton, DACIO, OCIO-IRMC
Maria Tinker, Executive Assistant, CIO, OCIO
Sarah Levin, Executive Assistant, ACIO, OCIO-IRMC
Sherry Golden, Agency Audit Liaison Official, OCIO-IRMC

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/resources/hotline-information

Cover photos are from USDA Flickr and are in the public domain. They do not depict any particular audit, inspection, or investigation.