U.S. Department of Labor
Office of Inspector General—Office of Audit

REPORT TO THE OFFICE OF THE CHIEF INFORMATION OFFICER

FY 2025 FISMA DOL INFORMATION SECURITY REPORT: EVALUATION OF DOL'S INFORMATION SECURITY PROGRAM

This report was prepared by KPMG LLP under contract to the U.S. Department of Labor, Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

Assistant Inspector General for Audit
U.S. Department of Labor

DATE ISSUED: MAY 27, 2026
REPORT NUMBER: 23-26-001-07-725

BRIEFLY...

FY 2025 FISMA DOL Information Security Report: Evaluation of DOL's Information Security Program

Why We Did the Audit

Under the Federal Information Security Modernization Act of 2014 (FISMA), the U.S. Department of Labor (DOL) Office of Inspector General (OIG) is required to perform annual independent evaluations of DOL's information security program and practices.

This effort assesses the effectiveness of information security controls over information resources that support federal operations and assets, and it provides a mechanism for improved oversight of information security programs. This includes assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

We contracted with KPMG LLP (KPMG) to conduct an independent performance audit on DOL's Fiscal Year (FY) 2025 information security program for the period of October 1, 2024, through June 30, 2025. To determine the effectiveness of the program, KPMG evaluated and tested security controls in accordance with applicable legislation, guidelines, directives, and other documentation.

What We Found

DOL's information security program continues to mature; however, certain insufficient cybersecurity controls are preventing DOL from maintaining an effective information security program. KPMG reported 14 findings for DOL's information security program. The findings were identified in 3 of 6 FISMA Cybersecurity Framework Functions and in 6 of the 10 FISMA Metric Domains. As a result, DOL's information security program was determined to be not effective, according to guidance from the Office of Management and Budget.

A security program is considered effective if the calculated score of the Cybersecurity Framework Functions is at least Managed and Measurable (Level 4). However, KPMG found weaknesses that demonstrated the information security program had not achieved a maturity rating of Managed and Measurable (Level 4) in three of the six FISMA Cybersecurity Framework Functions (Govern, Identify and Recover).

Specifically, KPMG found DOL's information security program did not fully adhere to applicable FISMA requirements, Office of Management and Budget policy and guidance, and National Institute of Standards and Technology standards and guidelines. KPMG noted deficiencies in the monitoring of DOL cloud service providers, multi-factor authentication enforcement, and the implementation of cybersecurity profiles. Furthermore, deficiencies were noted in user access provisioning and deprovisioning controls across systems within the DOL IT system portfolio.

As a result of the insufficiencies in DOL's information security program, DOL may face challenges in identifying and prioritizing cybersecurity risks effectively, which could lead to inadequate protection against cyber threats, increased vulnerabilities, and compromised data integrity. Furthermore, staffing vacancies and inadequate resources may result in a lack of oversight and effective operation of security controls and key IT processes, potentially impacting DOL's operational capabilities and compliance with federal cybersecurity mandates.

What We Recommended

KPMG made nine recommendations to strengthen DOL's information security program. KPMG also determined that eight prior year recommendations were closed, two remained open, and six were not submitted for closure by DOL management. DOL management concurred with the findings and recommendations.

Read the Full Report

For more information, go to: https://www.oig.dol.gov/public/reports/oa/2026/23-26-001-07-725.pdf.

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

Mangala Kuppa
Chief Information Officer
U.S. Department of Labor
200 Constitution Avenue NW
Washington, DC 20210

The U.S. Department of Labor (Department or DOL) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG), an independent certified public accounting firm, to conduct an audit of DOL's Fiscal Year (FY) 2025 information security program. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal Inspectors General, or an independent external auditor, to conduct annual evaluations of the information security program and practices of their respective agencies.

The OIG monitored KPMG's work to ensure it met professional standards and met contractual requirements. KPMG's independent audit was conducted in accordance with generally accepted government auditing standards.

KPMG was responsible for the auditors' evaluation and the conclusions expressed in the report while the OIG reviewed KPMG's report and supporting documentation.

Purpose

The objective of this audit was to determine if DOL implemented an effective information security program for the period of October 1, 2024, through June 30, 2025. The determinations in this report were based, in part, on the testing of a selection of DOL's entity-wide and system-specific security controls across 20 of its information systems. Additional details regarding the scope of the independent audit are included in KPMG's report.

Results

KPMG reported 14 findings for DOL's information security program. The findings were identified in 3 of 6 FISMA Cybersecurity Framework Functions and in 6 of the 10 FISMA Metric Domains. As a result, DOL's information security program

was determined to be "not effective" according to the Office of Management and Budget's guidance.

A security program is considered effective if the calculated score of the FY 2025 Core and Supplemental Inspector General Metrics reported in CyberScope[1] is at least Managed and Measurable (Level 4). KPMG found weaknesses that demonstrated the information security program had not achieved a maturity rating of Managed and Measurable (Level 4) in three of the six FISMA Cybersecurity Framework Functions: Govern, Identify, and Protect.

In determining DOL's FY 2025 assessed maturity level for each function, the OIG and KPMG performed a risk-based analysis leveraging the auditors' knowledge, the FY 2025 Core Metrics results, and the FY 2025 Supplemental Metrics results. The OIG and KPMG were not provided with any additional information during the audit or afterward to change this assessment.

KPMG performed testing on DOL networks to determine the operating effectiveness of data exfiltration and data loss prevention controls. Overall, DOL has controls in place to limit the unauthorized removal of sensitive Departmental or personally identifiable information; however, the controls were inconsistent across the selected agencies with varying levels of maturity and implementation.

In addition to the testing procedures performed for the FY 2025 Inspector General FISMA Reporting Metrics, KPMG performed additional procedures to determine the effectiveness of access controls—namely those associated with user access authorizations and the removal of access belonging to terminated or transferred users—across 87 additional systems and subsystems at DOL. Specifically, KPMG tested the effectiveness of user access provisioning and deprovisioning controls across the selected DOL information systems. Based on testing performed, KPMG noted deficiencies in adherence to DOL access provisioning and deprovisioning procedures across systems within the DOL IT system portfolio. These deficiencies included access that was not approved prior to provisioning and access that was not deprovisioned within the required timeframe after access was no longer needed.

KPMG found DOL's information security program did not fully adhere to applicable FISMA requirements, Office of Management and Budget policy and guidance, and National Institute of Standards and Technology standards and guidelines. KPMG noted deficiencies in the monitoring of DOL cloud service

[1] CyberScope, operated by the U.S. Department of Homeland Security on behalf of the Office of Management and Budget, is a web-based application designed to streamline information technology security reporting for federal agencies.

providers, multi-factor authentication enforcement, and the implementation of cybersecurity profiles.

KPMG made nine recommendations related to control deficiencies. After evaluating the implementation of recommendations from prior FISMA reports, KPMG determined eight recommendations were closed, two remained open, and six were not submitted for closure.

We appreciate the cooperation and courtesies the Office of the Chief Information Officer extended to us during this audit.

Laura B. Nicolosi
Assistant Inspector General for Audit

CONTRACTOR PERFORMANCE AUDIT REPORT

Independent Auditors' Performance Audit Report on the Effectiveness of the U.S Department of Labor's Information Security Program and Practices for Fiscal Year 2025

Chief Information Officer and Inspector General
U.S. Department of Labor
200 Constitution Avenue NW
Washington, DC 20210

We were engaged by the U.S. Department of Labor (Department or DOL) Office of Inspector General (OIG) to conduct a performance audit of the DOL information security program and practices for a selection of information systems. We conducted our performance audit with a scope 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 audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objectives. We believe 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. This report is prepared for the sole and intended use by DOL OIG.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to determine to what extent DOL implemented its information security program as established by the effectiveness of the relevant agency-wide and system-specific information system controls established in DOL's information security program. As such, we assessed relevant security controls and processes referenced in the six Cybersecurity Function areas outlined in the Fiscal Year (FY) 2025 Inspector General (IG) FISMA Reporting Metrics (herein referred to as the FY 2025 IG FISMA Reporting Metrics), which included Core Metrics and Supplemental Metrics. We tested relevant security controls referenced in Core Metrics and Supplemental Metrics and assessed the maturity levels on behalf of DOL OIG.

We performed data exfiltration testing over all networks within the Department, including the overall Department's network, DOL OIG, Bureau of Labor Statistics (BLS), and Job Corps networks[2] to determine if data exfiltration controls were operating effectively. We also followed up on the status of prior year recommendations. Additionally, we were engaged by DOL OIG to test access controls for a selection of 87 DOL systems and subsystems to determine if user access provisioning and deprovisioning for these systems adhered to DOL policies and procedures.

Based on the maturity levels calculated in CyberScope and Office of Management and Budget (OMB) guidance, we determined DOL's information security program was not effective. Within the context of the maturity model, OMB believes that achieving a Level 4 (Managed and Measurable) or above represents an effective level of security. For FY 2025, we determined the calculated average of the Core Metrics and Supplemental Metrics to assess the maturity levels of the Cybersecurity Framework Functions and overall information security program. Table 1 depicts DOL's assessed maturity levels for the five Cybersecurity Framework Functions in FY 2025.

Table 1: Maturity Levels for Cybersecurity Framework Functions

Cybersecurity Framework Functions	Maturity Level
Govern	Defined (Level 2)
Identify	Consistently Implemented (Level 3)
Protect	Managed and Measurable (Level 4)
Detect	Managed and Measurable (Level 4)
Respond	Managed and Measurable (Level 4)
Recover	Consistently Implemented (Level 3)
Overall	Consistently Implemented (Level 3)

Source: FY 2025 DOL CyberScope Response

During FY 2025, we tested security controls at the entity level and for a selection of 20 systems for each of the Cybersecurity Framework Functions. We identified 14 findings for DOL's information security program. The findings were identified in 3 of the 6 FISMA Cybersecurity Framework Functions and in 6 of the 10 FISMA Metric Domains. We considered the identified findings and relevant open prior year recommendations when we assessed the maturity levels for each of the Core Metrics and Supplemental Metrics, which were entered into the CyberScope reporting tool. In addition to testing security controls, we evaluated

[2] BLS, Job Corp, and the OIG are agencies within DOL but have separate networks from the rest of the Department. Separate data exfiltration testing was performed on each network.

the implementation of recommendations from prior information technology (IT) reports from 2019 through 2024. The IT reports included those prepared in connection with previous FISMA performance audits. Out of 16 previously open recommendations, we determined DOL successfully closed 8 recommendations. Based on the calculated score from CyberScope and OMB guidance, DOL's information security program was determined to be "not effective."

In response to these control deficiencies, we made nine new recommendations related to strengthening DOL's information security program. We suggest DOL implement a process to determine if these recommendations apply to other information systems. Furthermore, robust monitoring capabilities would enable DOL to continually assess the security state of its systems, including a process for identified compliance gaps.

We caution that projecting the results of our performance audit to future periods is subject to the risk that controls may become inadequate due to changes in conditions or because compliance with controls may deteriorate.

KPMG LLP

May 22, 2026

BACKGROUND

We conducted the FY 2025 FISMA performance audit under contract with DOL[3] in accordance with GAGAS. DOL OIG monitored our work to assess whether we met professional standards and contractual requirements.

Program Overview

DOL's Office of the Chief Information Officer (OCIO) operates within the Office of the Assistant Secretary for Administration and Management and as a customer service organization dedicated to providing IT solutions and leadership to advance DOL's missions. OCIO serves as the IT hub of DOL, and it develops, maintains, and protects IT solutions and data across the 27 DOL agencies to enable mission outcomes through technology and service. OCIO continually enhances the federal IT and digital capability with a focus on cybersecurity and customer experience to serve America's wage earners, job seekers, and retirees.

FISMA IG Metrics and Reporting

OMB and the Council of the Inspectors General on Integrity and Efficiency—with review and feedback provided by several stakeholders, including the Federal Chief Information Officers and Chief Information Security Officers councils—released OMB Memorandum M-25-04[4] to provide guidance for implementing the requirements outlined in the FY 2025 IG FISMA Reporting Metrics.

The FY 2025 IG FISMA Reporting 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. The Council of the Inspectors General on Integrity and Efficiency also maintained the maturity models for the 10 FISMA Metric Domains. Table 2 illustrates the alignment of NIST Cybersecurity Framework to the FISMA Metric Domains within the FY 2025 IG FISMA Reporting Metrics.

[3] DOL Contract Number: 1604DC-24-F-00017
[4] OMB Memorandum M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements (January 15, 2025), available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf

Table 2: Alignment of the NIST Cybersecurity Framework Functions to the FISMA Metric Domains

NIST Cybersecurity Framework Functions	FISMA Metric Domains
Govern	Cybersecurity Governance (CG) Cybersecurity Supply Chain Risk Management (C-SCRM)
Identify	Risk and Asset Management (RAM)
Protect	Configuration Management (CM) Identity and Access Management (IDAM) Data Protection and Privacy (DPP) Security Training (ST)
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning (CP)

Source: FY 2025 IG FISMA Reporting Metrics

In alignment with the FY 2025 IG FISMA Reporting Metrics v2.0,[5] the Core Metrics are to be evaluated annually, and the remaining metrics are to be evaluated on a 2-year cycle. The Core and Supplemental Metrics have been tailored to match the Administration's priorities and the priorities outlined in OMB Memorandum M-25-04. The FY 2025 IG FISMA Reporting Metrics included the following Core Metrics and Supplemental Metrics:

- Core Metrics
  - 5 - SCRM Processes
  - 7 - System Inventory
  - 8 - Hardware Inventory
  - 9 - Software Inventory
  - 11 - Enterprise Risk Management & Risk Assessments
  - 12 - Risk Management Dashboards and Reporting
  - 14 - Configuration Settings
  - 15 - Flaw Remediation
  - 17 - Multi-factor Authentication (MFA) - General Users
  - 18 - MFA - Privileged Users

[5] FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0 (April 3, 2025), available at: https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508.pdf

  - 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 Test, Training, and Exercise
- Supplemental Metrics
  - 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 Scoring

The ratings in the 10 FISMA Metric Domains identified in Table 2 (CG, C-SCRM, RAM, CM, IDAM, DPP, ST, ISCM, IR, and CP) were determined by a calculated average of the assessed maturity levels based on the aforementioned maturity model, as well as qualitative and quantitative measures used to make risk-based determinations of the overall security program.[6] When maturity levels were entered into the CyberScope reporting tool, the tool automatically calculated the average of the Core Metrics and Supplemental Metrics for each FISMA Metric Domain and Cybersecurity Framework Function. The maturity model has five levels. Table 3 details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework Function.

[6] The calculated averages were not automatically rounded up or down, as other data points were used to make a risk-based determination of the overall program.

Table 3: Inspector General Assessed Maturity Levels

Maturity Level	Description
Ad Hoc (Level 1)	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Defined (Level 2)	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Consistently Implemented (Level 3)	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable (Level 4)	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.
Optimized (Level 5)	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.

Source: FY 2025 IG FISMA Reporting Metrics

According to the FY 2025 IG FISMA Reporting Metrics, OMB believes that achieving a Level 4 (Managed and Measurable) rating or above represents an effective level of security. For FY 2025, a calculated average scoring model was used, and the 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 purpose of assessing maturity levels for each metric is to drive continued improvements in cybersecurity maturity across the federal environment and specific agency efforts.

In addition to conducting the testing necessary to respond to the FISMA metric questions, we performed two separate additional testing scenarios: (1) data exfiltration testing on four general support systems at DOL, the OIG, BLS, and Job Corps and (2) additional Access Control testing for 87 of 201 systems and subsystems in DOL's IT system inventory.[7] See Appendix A for more details.

[7] DOL's IT system inventory includes the listing of all DOL systems and subsystems from the Cybersecurity Assessment Management tool, including both FISMA and non-FISMA reportable systems, as of April 10, 2025.

RESULTS

Based on the ratings for each FY 2025 IG FISMA Reporting Metric and associated averages calculated in CyberScope, we determined DOL's information security program was not effective. DOL did not achieve an overall rating of Level 4 (Managed and Measurable) because it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. According to OMB, an agency's security program is considered effective if the calculated average of the Core Metrics and Supplemental Metrics are at least Managed and Measurable (Level 4). Table 4 depicts the maturity levels determined for the six Cybersecurity Framework Functions and their corresponding FISMA Metric Domains.

Table 4: FY 2025 Cybersecurity Framework Function Maturity Levels

Cybersecurity Framework Functions	Maturity Level
Govern – CG and C-SCRM	Defined (Level 2)
Identify – RAM	Consistently Implemented (Level 3)
Protect – CM, IDAM, DPP, and ST	Managed and Measurable (Level 4)
Detect – ISCM	Managed and Measurable (Level 4)
Respond – IR	Managed and Measurable (Level 4)
Recover – CP	Consistently Implemented (Level 3)

Source: FY 2025 DOL CyberScope Response

For each of the Cybersecurity Framework Functions, we identified weaknesses, strengths, and areas for improvement. In areas with weaknesses, we issued findings to DOL with recommendations to improve their processes. Additionally, we assessed prior year recommendations to determine whether remediations that were implemented satisfied the recommendation (see Appendix C).

In the CG function area, DOL should develop and implement a process to create and monitor current and target cybersecurity profiles to enable the Department and external stakeholders to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives. Additionally, DOL OCIO lost a significant amount of federal personnel and contracting support, which led to gaps in governance responsibilities and inaccurate cybersecurity points-of-contact in DOL's cybersecurity governance, risk, and compliance system.

Within the C-SCRM function area, DOL should enhance its cloud service provider monitoring procedures. Findings in this area revealed that DOL is not identifying and reviewing service provider deliverables in a timely and accurate manner. This prevents them from gaining insight into risks and vulnerabilities within their service providers' services.

We noted multiple instances in which DOL demonstrated effective controls, including a robust information system continuous monitoring capability whereby data was gathered from component agencies within the Department and compiled into a centralized monthly review, which enables risk decisions to be made. DOL defined key performance objectives to which component agencies are held and aggregated risk scores for senior leaders to make decisions for individual systems and agencies. Additionally, DOL has a robust incident response program that captures incidents from across the Department, triages, categorizes, and coordinates with various offices in DOL and outside organizations to support the remediation of outstanding incidents. DOL has multiple supporting tools and applications to assist with triaging and tracking cybersecurity incidents, including an incident database, Splunk,[8] Microsoft Defender, and other cybersecurity tools.

We have also identified opportunities to improve that, if effectively implemented, would help DOL to reach Managed and Measurable (Level 4), which, according to OMB, reflects an effective information security program. For example, multiple applications and one general support system within DOL are not utilizing MFA and solely rely on username and password to authenticate DOL or external users to the application.

We also evaluated the implementation of recommendations from prior IT reports from 2019 through 2024. The IT reports included those prepared in connection with previous FISMA performance audits. Out of 16 previously open recommendations, we determined DOL successfully closed 8 recommendations.

In the following sections, we describe each Cybersecurity Framework Function and domain with an overview of the testing results, which noted specific strengths and weaknesses.

Govern

The objective of the Cybersecurity Framework's Govern Function is to establish and oversee DOL's cybersecurity risk management strategy, expectations, and

[8] Splunk is a software platform that allows organizations to collect, search, monitor, and analyze machine-generated data from a variety of sources, such as websites, applications, sensors, and devices.

policies, ensuring cybersecurity is integrated with business objectives and risk management processes.

We assessed DOL's Govern function as Defined (Level 2) because OCIO: (1) does not have a process to develop and implement current and target cybersecurity profiles, (2) had inaccurate cybersecurity governance responsibilities and points-of-contact, and (3) did not perform continuous monitoring on cloud service providers.

Cybersecurity Governance

The CG domain requires federal agencies to provide oversight to the cybersecurity program and communicate organizational cybersecurity objectives to relevant internal and external stakeholders.

Based on the results of our performance audit procedures, we assessed DOL's CG FISMA Metric Domain as Defined (Level 2). OCIO implemented a cybersecurity risk management strategy to support operational risk decisions, utilize qualitative and quantitative performance measures and allow senior leadership to provide oversight and accountability across the Department. However, OCIO did not define a formal process for developing and maintaining current and target cybersecurity profiles. Cybersecurity profiles, as defined by NIST Cybersecurity Framework 2.0,[9] are used to understand, tailor, assess, prioritize, and communicate the Core Metric's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

DOL lost significant federal staff and contract support during FY 2025. The large number of departures led to significant vacancies within OCIO, including system owners, Department and branch leads, and other positions of authority. OCIO adjusted quickly to the departures by reorganizing, downsizing departments, and shifting assignments; however, key position vacancies remained.

Cybersecurity Supply Chain Risk Management

C-SCRM requires agencies to develop policies, procedures, and programs to manage supply chain risks associated with systems' development, acquisition, maintenance, and disposal. This includes monitoring third-party vendors and service providers to assess whether appropriate contractual requirements are included for acquisitions.

[9] The NIST Cybersecurity Framework (CSF) 2.0 (February 26, 2024), available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Based on the results of our performance audit procedures, we assessed DOL's SCRM FISMA Metric Domain as Defined (Level 2). OCIO developed and implemented SCRM standards and procedures to assess supply chain risks associated with suppliers and contractors. However, OCIO did not sufficiently perform annual assessments of cloud service providers to assess whether controls of systems or services provided by contractors complied with FISMA requirements. In addition, the monthly continuous monitoring program for cloud service providers was ineffective because control operators did not follow defined procedures to identify and follow up on deficient deliverables. Specifically, a DOL service provider was suspended from the Federal Risk and Authorization Management Program (FedRAMP) marketplace for failing to provide various monitoring deliverables, and DOL did not timely identify the suspension or perform reauthorization procedures.

Identify

The objective of the Cybersecurity Framework's Identify Function is to manage cybersecurity risk to the systems, people, assets, data, and capabilities of DOL. When an agency understands the cybersecurity risks that threaten its mission and services, it can establish controls and processes to manage and prioritize risk management decisions.

We assessed DOL's Identify Function as Consistently Implemented (Level 3). OCIO had multiple inaccuracies within their Cybersecurity Assessment Management (CSAM)[10] tool.

Risk and Asset Management

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. RAM is the process of identifying, assessing, and controlling threats to an organization's operating environment. These threats or risks could stem from a wide variety of sources, including budget uncertainty, natural disasters, and cybersecurity threats. A sound RAM plan and program can provide impactful information to an agency when establishing an information security program.

Based on the results of our performance audit procedures, we assessed DOL's RAM FISMA Metric Domain as Consistently Implemented (Level 3). OCIO

[10] CSAM is designed to help federal agencies streamline their compliance and security processes. CSAM empowers federal agencies with an end-to-end Assessment and Authorization (A&A) application providing automated inventory, configuration, and vulnerability management.

implemented policies and procedures to maintain a complete and accurate inventory of its major information systems, hardware devices, and software, but it has not implemented a system of record to maintain a Department-wide comprehensive data inventory to account for all data assets created, collected, or maintained by DOL. OCIO also utilized automated tools to manage its software and hardware assets and to provide real-time visibility into assets connected to the DOL network. In addition, OCIO has a centralized, enterprise view of cybersecurity risks across the organization using the CSAM tool and a Cybersecurity Risk Management Committee to manage cybersecurity risk.

OCIO used the CSAM tool as the primary source to authorize information systems, obtain risk data, and maintain the official system inventory. DOL stakeholders used these processes to identify, manage, and track cybersecurity risks in an official Cybersecurity Risk Response tracking system, which included pending and approved risk responses. The Cybersecurity Risk Response tracking system was integrated into DOL's Enterprise Risk Register to include risks that OCIO considered based on the operation and use of its information systems and the variability of environments that exist within DOL. DOL management and the Cybersecurity Risk Management Committee discussed risks and assigned qualitative and quantitative data points to each risk to support the prioritization of risks and to enable decision-making.

OCIO identified and categorized its information systems according to their priority in enabling the agency mission and business functions. Prioritization was performed through a risk-driven allocation of resources based on system categorization. OCIO also implemented an asset value scoring system to calculate scores for each information system by aggregating information stored in the CSAM tool and to identify high value assets needed for DOL to meet its mission essential functions.

In accordance with OMB Memorandum M-25-05,[11] DOL should work to implement a Department-wide comprehensive data inventory to account for all data assets created, collected, or maintained by DOL by September 30, 2026.

Finally, multiple findings were identified within the CSAM tool, including inaccurate system points-of-contact, retired systems linked to active systems as interconnections, and inaccurate system categorization. CSAM is used as the system of record for risk management, and inaccurate data can lead to inappropriate or misguided decisions.

[11] OMB Memorandum M-25-05, Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance (January 15, 2025), available at: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-05-Phase-2-Implementation-of-the-Foundations-for-Evidence-Based-Policymaking-Act-of-2018-Open-Government-Data-Access-and-Management-Guidance.pdf

Protect

The objective of the Cybersecurity Framework's Protect Function is to develop and implement appropriate safeguards to enable the delivery of critical services by DOL. The Protect Function supports the ability of DOL to limit, contain, or prevent the impact of a cybersecurity event. We assessed DOL's Protect Function as Managed and Measurable (Level 4). While DOL implemented policies and procedures for CM, IDAM, DPP, and ST, our testing found deficiencies associated with the implementation and effectiveness of controls in the IDAM and DPP FISMA Metric Domains.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures to enable compliance with minimally acceptable system configuration requirements. CM refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations.

Based on the results of our performance audit procedures, we assessed DOL's CM FISMA Metric Domain as Managed and Measurable (Level 4). OCIO implemented and communicated an enterprise-wide CM plan, which defines roles and responsibilities of CM stakeholders. The CM process allocated resources in a risk-based manner, and OCIO captured qualitative and quantitative performance measures of effectiveness for its configuration management plan using automated and centralized tools.

Furthermore, OCIO implemented automated tools to assess the baselines and configurations settings of its information systems. These tools enabled near real-time monitoring of its information systems and the ability to generate reports of compliant and non-compliant devices. However, one DOL agency that was partially serviced, DOL OIG, did not implement a process to remediate deviations from information system baselines timely.

OCIO centrally managed its flaw remediation process. It also monitored, analyzed, and reported the qualitative and quantitative performance measures of effectiveness for its flaw remediation processes using automated tools and technologies. OCIO implemented controls to enable compliance with timelines for remediating vulnerabilities and to implement or track such remediations accordingly.

Identity and Access Management

The IDAM Domain includes the requirement that an agency must implement a set of capabilities to help ensure users authenticate to and only have access to IT resources that are required for their job function—a concept referred to as "need to know." 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.

Based on the results of our procedures, we assessed DOL's IDAM FISMA Metric Domain as Consistently Implemented (Level 3). OCIO developed and implemented IDAM policies and procedures, and our testing found issues in OCIO's implementation and operating effectiveness of defined IDAM security controls.

OCIO configured most of its information systems to require strong authentication mechanisms for privileged and non-privileged users; however, we identified multiple findings relating to the use of MFA. We did note that DOL implemented additional automated mechanisms to support the use and management of privileged user accounts, to include the logging and review of privileged user actions and ensuring segregation of duties. OCIO has implemented the CyberArk[12] tool to assist with privileged user management.

We were engaged to perform an audit of DOL's consolidated financial statements for FY 2025. During the audit and as of April 24, 2026, we issued notices of findings and recommendations to the Department in the following areas:

- untimely removal of users from in-scope financial applications and supporting production database after separation from the agency;
- untimely removal of users from an in-scope financial applications after the user access reauthorization process;
- lack segregation of duties between developers and change migrators in the change management process for an in-scope financial application, supporting databases, and a supporting tool; and
- users of financial applications reviewing their own access during the annual user access reauthorization processes.

The audit is currently ongoing.

[12] CyberArk is a third-part privileged access management tool that allows DOL to centrally manage privileged access to services across the Department and offers critical services.

During our fieldwork, we also performed additional access control testing across a selection of 87 out of 201 systems and subsystems. We found that two systems did not follow policies and procedures for provisioning user access and three systems did not follow policies and procedures for deprovisioning user access. Supporting documentation, including system generated user listings and user access forms, was unavailable for 12 systems; thus, we determined that the controls were not operating effectively.

In addition to the testing above, we examined recommendations made in prior financial statement audits. We determined management had 10 prior year open financial statement audit recommendations related to our findings in this audit.

Data Protection and Privacy

DPP refers to a collection of activities focused on the security objective of confidentiality, the preservation of authorized restrictions of information access, and the protection of improper disclosure of personal privacy and proprietary information. Effectively managing the risks associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) increasingly depends on the safeguards employed for systems that process, store, and transmit such information. Accordingly, OMB Circular A-130,[13] requires federal agencies to develop, implement, and maintain agency-wide privacy programs that, where PII is involved, play a key role in information security and the proper implementation of the NIST Risk Management Framework. Although the head of each federal agency remains ultimately responsible for ensuring privacy interests are protected and managing PII responsibly, Executive Order 13719[14] requires agency heads to designate a Senior Agency Official for Privacy who is accountable for the agency's privacy program.

Based on the results of our procedures, we assessed DOL's DPP FISMA Metric Domain as Consistently Implemented (Level 3). DOL had processes and technology in place to protect the confidentiality, availability, integrity and availability of its data through encryption at rest and in transit, monitoring, and through backups of data; however, controls put in place were inconsistently effective, including, for example, the use of removable media without authentication or encryption.

[13] OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016), available at: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
[14] Executive Order 13719, Establishment of the Federal Privacy Council (February 9, 2016), available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council

In addition to testing procedures performed in accordance with the FY 2025 IG FISMA Reporting Metric questions, we conducted additional tests to determine the effectiveness of data exfiltration and data loss prevention controls. As part of our approach, we performed data exfiltration testing against DOL, DOL OIG, Job Corps, and BLS networks. Test cases included attempting to send fictitious PII outside of the network through various means;[15] using publicly available artificial intelligence (AI) platforms, such as ChatGPT, to manipulate PII data; and attempting to infill and exfil fictious data through removeable media. Our testing produced varying results across the agencies. Selected agencies did not block the use of publicly available AI platforms. OCIO, the OIG, and BLS did not block the transfer of PII through email but did generate alerts through data loss prevention tools. BLS did not prevent the infill or exfil of data using removeable media. Overall, DOL had inconsistent controls preventing the exfiltration of data with varying levels of maturity and implementation.

Security Training

ST is a cornerstone of a strong information security program as regular IT users and privileged users must have the knowledge to perform their jobs appropriately while using information system resources without exposing the organization to unnecessary risk.

Based on the results of our procedures, we assessed DOL's ST FISMA Metric Domain as Managed and Measurable (Level 4). OCIO integrated security awareness and training activities throughout DOL and utilized multiple security-related domains to relay key information security messaging.

OCIO monitored performance measures of effectiveness for its security awareness and training strategies, plans, and programs by capturing course evaluation statistics, conducting phishing exercises and analyzing associated results, promoting social media campaigns, and updating training based on feedback received from users and evolving threats and risks.

Detect – Information Security Continuous Monitoring

The objective of the Cybersecurity Framework's Detect Function is to implement activities to identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework advises that continuous monitoring processes be

[15] During testing, we attempted to send PII through email, Microsoft Teams messages, and other file sharing mechanisms.

used to detect anomalies and changes in the organization's environment of operation and to maintain knowledge of threats and security control effectiveness.

Based on the results of our procedures, we assessed DOL's Detect Function and the aligned ISCM FISMA Metric Domain as Managed and Measurable (Level 4). OCIO implemented ISCM policies and procedures for monitoring at various organizational tiers and documented and communicated ISCM roles and responsibilities through the DOL ISCM plan.

OCIO's ISCM program facilitated the Ongoing Authorization process, as well as the collection of security-related information related to, among other things, risk management, contingency planning, vulnerability management, and identity and access management in ISCM compliance review reports. These reports included performance metrics to measure the effectiveness across the domain areas. OCIO utilized system security-related information in the ISCM monitoring. This enabled the effective operation of its systems through the Ongoing Authorization process within DOL's risk tolerance.

Respond – Incident Response

The objective of the Cybersecurity Framework's Respond Function is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing IR plans and procedures, analyzing security events, and effectively communicating IR activities. FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for IR.

Based on the results of our procedures, we assessed DOL's Respond Function and the aligned IR FISMA Metric Domain as Managed and Measurable (Level 4). OCIO implemented policies and procedures for incident detection, handling, and analysis. OCIO also implemented automated tools, such as threat analytics dashboards, incident review dashboards, and malware analysis, to monitor and trigger alerts to potential incidents. These tools fed into DOL's Security Information and Event Management solution to offer stakeholders a centralized view of the incidents. Additionally, OCIO collaborated with the U.S. Department of Homeland Security (DHS) and utilized the tools of DHS to proactively block cyber-attacks and prevent potential compromises. This technical assistance was leveraged to improve IR support.

OCIO utilized its threat vector taxonomy to classify incidents and capture metrics for the incidents reported in accordance with U.S. Computer Emergency Readiness Team guidelines. Additionally, OCIO captured and used information about the impact of incidents to mitigate related vulnerabilities in other systems.

Recover – Contingency Planning

The objective of the Cybersecurity Framework's Recover Function is to help ensure organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines CP processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event.

Based on the results of our procedures, we assessed DOL's Respond Function and the aligned CP FISMA Metric Domain as Consistently Implemented (Level 3). OCIO implemented policies and procedures to enable the maintenance and execution of its CP. Furthermore, OCIO established CP roles and responsibilities throughout the organization.

OCIO used Business Impact Analyses and CP tests and exercises to support CP processes and help ensure critical infrastructure and systems were able to support timely recovery and reduce the impact of a cybersecurity incident. However, the risk scoring from the Business Impact Analysis was stored in CSAM, which had multiple inaccuracies, and DOL did not define the requirement to perform functional contingency planning tests.

AUDIT FINDINGS AND RECOMMENDATIONS

As a result of our work, we identified 14 findings and made 9 new recommendations. OCIO's focus on continuous improvement, including addressing open prior year recommendations, and its implementation of new technologies will help make its program more effective and enable DOL to achieve higher maturity levels.

Govern – Cybersecurity Governance

Finding 1: Lack of Cybersecurity Profiles

DOL management indicated that cybersecurity profiles were defined by the DOL Cybersecurity Policy Portfolio (CPP). The DOL CPP is a set of IT security policies and does not meet the definition of a cybersecurity profile as described by the NIST Cybersecurity Framework. Thus, DOL did not define a formal process for developing and maintaining current and target cybersecurity profiles.

According to NIST Cybersecurity Framework 2.0, cybersecurity profiles are defined as an organization's current and/or target cybersecurity posture in terms of the Cybersecurity Framework Core's outcomes. Organizational profiles are used to understand, tailor, assess, prioritize, and communicate the Cybersecurity Framework Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders. Additionally, the FY 2025 IG FISMA Reporting Metric CG-1 states that agencies should have a process to create and update cybersecurity profiles.

DOL did not perform an adequate risk assessment, and it did not understand the definition of a cybersecurity profile as defined by NIST Cybersecurity Framework 2.0. Furthermore, DOL did not identify the need to define their current and target cybersecurity profiles to internal and external stakeholders. As of February 2024, cybersecurity profiles were required in NIST Cybersecurity Framework 2.0.

The absence of a formal process for developing and maintaining current and target cybersecurity profiles, as outlined in NIST Cybersecurity Framework 2.0, exposes DOL to increased risks associated with effectively identifying and prioritizing cybersecurity risks, leading to potential misalignment of security measures with business objectives. This in turn could result in the inadequate establishment of protection measures to counter threats, increased vulnerability to data breaches, and potential non-compliance with regulatory requirements, ultimately compromising DOL's operational integrity and reputation.

We recommend the Chief Information Officer (CIO):

1. Develop and implement a process to create and maintain target and current cybersecurity profiles.

Finding 2: CSAM Inaccuracies

We found OCIO did not update system owners within CSAM for 2 of 15 systems selected for testing. The system owners listed had left the Department, and CSAM had not been updated to reflect the vacancy or replacement. Furthermore, OCIO did not accurately list interconnections in the System Security Plan for 1 of 15 systems selected for testing. Specifically, the System Security Plan was not updated to reflect the removal of a retired Office of the Assistant Secretary for Administration and Management system and listed the retired system as an active system interconnection.

According to the DOL CPP, DOL should include:

> resources needed to implement the information security and privacy programs in capital planning and investment requests, document all exceptions to this requirement, and prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.[16]

In addition, per the DOL CPP, DOL should approve and manage the exchange of information between systems using the system security plan.[17]

We found that reductions in staffing, increasing workloads, and changing staff assignments caused delays in making updates to CSAM and its System Security Plan. OCIO management also informed us that the relationship information within CSAM was populated with outdated interconnection data, which led to a retired system being listed as an active system interconnection.

Inaccurate information within the risk management system of record may lead to inefficient operational processes and hinder effective risk management strategies or could result in security controls being applied inappropriately.

We recommend the CIO:

2. Develop and implement controls to validate information within the Cybersecurity Assessment Management tool.

Govern – Cybersecurity Supply Chain Risk Management

Finding 3: Ineffective Cloud Service Provider Monitoring

OCIO did not timely identify that a Software as a Service cloud service provider was not providing various continuous monitoring deliverables, including security control assessments, vulnerability scans, and plan of action and milestone documents, to verify the security status of their service.

[16] DOL CPP, Volume 18: Program Management (PM), section 2.3, PM-3: Information Security and Privacy Resources
[17] DOL CPP, Volume 4: Assessment, Authorization, and Monitoring (CA), section 2.3, CA-3: Information Exchange

According to the DOL CPP, for cloud products and services, the cloud service provider's implementation of FedRAMP continuous monitoring satisfies continuous monitoring for cloud service provider-implemented controls.[18]

The finding occurred because OCIO did not review continuous monitoring deliverables from cloud service providers through FedRAMP.

Without a suitably designed and effective continuous monitoring process for cloud service providers, DOL may not identify cloud system vulnerabilities in a timely manner, thereby increasing risk to the confidentiality, availability, and integrity of DOL data.

We did not provide a new recommendation as this finding is related to the following open prior year recommendation:

- Develop and implement an unambiguous standard operating procedure, utilizing Federal Risk and Authorization Management Program guidance and leading practices, to monitor cloud service providers and escalate noncompliance effectively to the agency Authorizing Official, including defined risk management deficiency triggers.
  (FY 2024, Recommendation 1)

Identify – Risk and Asset Management

Finding 4: Interconnection Service Agreements Not Being Reviewed

The OIG did not perform a review of the interconnection service agreement between an OIG system and an Office of the Assistant Secretary for Administration and Management system. The CPP requires Information System Security Officers to review interconnection service agreements between information systems every 5 years or after significant system changes. The interconnection service agreement between these two systems had not been reviewed since it was signed in 2009.

According to the DOL CPP, DOL should approve and manage the exchange of information between systems and other systems using the system security plan and, for external systems, other agreements (e.g., memorandum of understanding, interconnection security agreement, and contracts). The

[18] DOL CPP, Volume 4: Assessment, Authorization, and Monitoring (CA), section 2.7, CA-7: Continuous Monitoring

Information System Security Officer should review and update the agreements every 5 years or after significant system changes.[19]

The OIG did not implement a defined process for the review and oversight of interconnection service agreements on a routine basis, which resulted in the interconnection service agreement not being reviewed for 15 years. The OIG stated it never had a process or control in place to ensure adherence to the CPP requirement for interconnection agreement reviews.

The finding increases the risk that ineffective decision-making based on outdated interconnection service agreements hinders effective risk management strategies and/or results in the inconsistent and/or inappropriate application of security controls.

We recommend DOL OIG:

3. Implement a control to help ensure that all interconnection service agreements or related documents are reviewed in accordance with the DOL Cybersecurity Policy Portfolio.

Finding 5: Improper System Categorization

We found BLS did not properly categorize seven systems within its CSAM system inventory. These seven systems were categorized as “non-FISMA reportable” when they should have been designated as “FISMA reportable” or as “subsystems of a FISMA reportable system.”

According to the DOL CPP, DOL’s information systems inventory, for purposes of FISMA, is designated in CSAM.[20] It constitutes all System Types designated as “Systems” that are considered federal systems.

Through a root cause analysis, BLS determined that these systems were categorized as “non-FISMA reportable” by DOL when they were established in CSAM. Prior to CSAM, BLS relied on paper documentation, and these systems were also categorized as “minor systems” at that time under the former DOL IT policy and guidance. DOL recently removed the minor system designations, though the “non-FISMA reportable” categorization remained.

Improper system categorizations can lead to inadequate controls identification and implementation and information system continuous monitoring, thereby

[19] DOL CPP, Volume 4: Assessment, Authorization, and Monitoring (CA), section 2.3, CA-3: Information Exchange
[20] DOL CPP, Volume 18: Program Management (PM), section 2.5, PM-5: System Inventory

increasing the risk of the degradation of the integrity, confidentiality, and availability of the system and underlying data.

We did not provide a new recommendation as this finding is related to another current finding, Finding 2, and has the same recommendation:

- Develop and implement controls to validate information within the Cybersecurity Assessment Management tool.

Finding 6: Lack of Defined Policies and Procedures for Maintaining an Inventory of Data

DOL did not define its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of data and corresponding metadata for its data types, including data obtained from third party providers, as appropriate. DOL has drafted an internal document that outlined data management leading practices, but DOL agencies were not required to follow it.

In accordance with OMB Memorandum M-25-05, DOL should develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by DOL.

Due to changes in the Department's priorities and reduced resources, DOL has placed a program to create and implement a Department-wide inventory of data on hold; however, implementation of a comprehensive data inventory is not required until September 30, 2026.

Because the implementation of a comprehensive data inventory is not required to be fully implemented until September 30, 2026, we have not provided a recommendation to the CIO.

Protect – Configuration Management

Finding 7: Baseline Deviation Process

The OIG did not design a formal process to monitor and track the remediation of security configuration baseline deviations in a timely manner for the OIG system.

According to the DOL CPP, the OIG should identify, document, and approve any deviations from established configuration settings for system hardware, software,

or firmware components based on explicit operational requirements.[21] However, due to competing priorities and a lack of resources, we determined that the OIG was not routinely monitoring the BigFix Compliance scanning tool.[22]

The OIG faces a security risk of prolonged exposure to vulnerabilities, as deviations from security baselines may go unaddressed. Consequently, the OIG system could be more susceptible to unauthorized access, data breaches, and other cyber threats, potentially compromising the integrity, confidentiality, and availability of critical information resources. This lack of oversight may also hinder the OIG's ability to comply with regulatory requirements and cybersecurity leading practices, further exacerbating the risk.

We recommend DOL OIG:

4. Implement a baseline deviation monitoring process for its general support system.

Protect – Identity and Access Management

Finding 8: Lack of Multi-factor Authentication

We found 4 of 20 DOL information systems selected for testing, which included three applications and one general support system, were not configured to enforce MFA.

For two applications, DOL determined that the system was developed prior to federal requirements mandating the implementation of MFA to all layers of technology. Furthermore, OCIO did not prioritize major system upgrades, as the system was planned to be disposed of and replaced. For the other application, it was determined that the OIG did not understand the requirements of Executive Order 14028,[23] which requires MFA at each layer of technology and does not allow entities to rely solely on the network layer to meet MFA requirements.

Finally, for the OIG system, it was determined the OIG did not adequately plan for alternative means for MFA applicable to privileged access after OCIO removed the OIG's ability to authenticate its privileged accounts through

[21] DOL CPP, Volume 5: Configuration Management (CM), section 2.6, CM-6: Configuration Settings
[22] BigFix Compliance is a security compliance management software suite that enables organizations to scan their end points against a wide-variety of security hardening guides to ensure end point compliance in-line with policies and procedures.
[23] Executive Order 14028, Improving the Nation's Cybersecurity (May 12, 2021), available at: https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

Personal Identification Verification (PIV) cards. We were informed that this decision was due to guidance changes from the DOL security badging office.

Per Executive Order 14028, agencies needed, within 180 days of the order's issuance, to adopt MFA and encryption for data-at-rest and in transit to ensure consistency with federal records laws and other related laws. Furthermore, according to OMB Memorandum M-22-09,[24] "MFA should be integrated at the application layer, such as through an enterprise identity service…rather than through network authentication (e.g., a virtual private network)." In addition, the DOL CPP states, "MFA for access to system-specific non-privileged accounts must be through a two-factor PIV credential or other IAL3/AAL3 credential."[25]

The absence of MFA increases the risk of unauthorized access through compromised credentials as single factor authentication is significantly easier to breach. This could result in unauthorized access, misuse, or mishandling of DOL applications and data.

We did not provide a new recommendation as this finding is related to the following open prior year recommendation:

- Complete in progress efforts to modernize impacted systems and subsequently enable MFA. (FY 2024, Recommendation 3)

Finding 9: Lack of Session Timeout for System

We found OCIO did not configure 1 of 15 systems to enforce session timeouts after 30 minutes of inactivity in accordance with the DOL CPP.

According to the DOL CPP, DOL should configure all systems to automatically terminate a user session after 30 minutes of inactivity.[26]

After performing a root cause analysis, DOL determined that it did not procure a version of the commercial-off-the-shelf application that complied with the DOL CPP requirement for session timeouts.

The absence of a session timeout control increases the risk that an unauthorized user could obtain system access through a stale session. This could result in unauthorized access, misuse, or mishandling of DOL applications and data.

[24] OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022), available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[25] DOL CPP, Volume 7: Identification and Authentication (IA), section 2.2.1, Control IA-2(1): Multi-Factor Authentication to non-Privileged Accounts
[26] DOL CPP, Volume 1: Access Controls (AC), section 2.12: AC-12: Session Timeouts

We recommend the CIO:

5. Ensure all systems comply with the Cybersecurity Policy Portfolio requirements for session timeouts.

Finding 10: Missing Audit Log Review

The OIG did not provide documentation to substantiate the completion of a system audit log review for one of two selected months for 1 of 15 systems selected for testing, as required by the system security plan.

In accordance with the system's system security plan, Control AU-6, Audit Record Review Analysis and Reporting, the OIG reviews the information system audit records collected monthly by Splunk for indications of viewing, downloading, accessing, searching for, transferring, sharing, storing, creating, sending, or providing access to any type of restricted or inappropriate material, messages, or content.

The OIG did not collect the corresponding evidence for the January 2025 audit log review, and the person responsible for the review has since left the Department.

The finding increases the risk of undetected security incidents, as the absence of audit log reviews may allow unauthorized access or malicious activities to go unnoticed. Consequently, the OIG's general support system and its production data may be exposed to potential threats, compromising the integrity, confidentiality, and availability of critical information.

We did not provide a new recommendation as this finding is related to the following open prior year recommendation:

- Assign appropriate resources to perform the audit log reviews as required by the system security plan. (FY 2024, Recommendation 5)

Finding 11: Logical Access Controls Not Operating Effectively

We found 5 systems out of a selection of 87 systems did not have effective access controls.

DOL management's user provisioning controls were not operating effectively for two systems. Specifically, management established user accounts on these systems before receiving approved user access forms. Additionally,

management's user deprovisioning controls were not operating effectively for three systems. Management did not remove the user accounts after the users' access was no longer required.

According to the DOL CPP, access is required to be documented and approved prior to being provisioned. Additionally, once it is identified that an employee no longer needs access to a specific system, access is to be removed within 10 business days for a voluntary employee action or 4 hours for an involuntary employee action.[27]

DOL did not provide an appropriate level of management oversight due to the large amount of personnel changes and did not enforce effective logical access procedures and controls.

The absence of logical access controls increases the risk that an unauthorized user obtains system access. This could result in unauthorized access, misuse, or mishandling of DOL applications and data.

We recommend the CIO:

6. Ensure the adherence to DOL logical access policies and procedures.

7. Establish mechanisms to ensure that logical access controls are implemented and effective.

Finding 12: Evidence Not Provided Timely

During the additional access controls testing, DOL was unable to provide system generated user listings and user access forms for 12 of 87 selected systems during the performance audit period. Therefore, we were unable to determine whether the access provisioning and deprovisioning controls were designed and operating effectively for these systems.

The Government Accountability Office's (GAO) Standards for Internal Control in the Federal Government,[28] Principle 3, states that 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

[27] DOL CPP, Volume 1: Access Control (AC) Standards and Procedures, section 2.2, AC-2 Account Management
[28] GAO, Standards for Internal Control in the Federal Government, GAO-25-107721 (May 15, 2025), available at: https://www.gao.gov/products/gao-25-107721

to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

Furthermore, according to the DOL CPP, access is required to be documented and approved prior to being provisioned. Additionally, once it is identified that an employee no longer needs access to a specific system, access is to be removed within 10 business days for a voluntary employee action or 4 hours for an involuntary employee action.[29]

Without audit trails or supporting documentation, management does not have assurance that user access was appropriately authorized or removed, as a result of employee/contract termination or transfer.

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 DOL's logical access control environment.

We recommend the CIO:

8. Design and implement a process to ensure identity and access management internal control documentation is retained to support its system of internal controls and operational needs, as required by Government Accountability Office's Standards for Internal Control in the Federal Government.

Protect – Data Protection and Privacy

Finding 13: Data Loss Prevention Tools Not Configured Properly

The OIG did not configure its data loss prevention tools to prevent users from removing data from the OIG network on to removable media, such as a Universal Serial Bus (USB) device. As a result, an employee was able to move files from their workstation to a personal USB device without being prompted to encrypt the device or being prevented from copying the data.

According to the DOL CPP, the Department should protect and control both digital and/or non-digital media containing Controlled Unclassified Information during transport outside of controlled areas using cryptographic mechanisms and/or locked containers.[30]

[29] DOL CPP, Volume 1: Access Control (AC) Standards and Procedures, section 2.2, AC-2 Account Management
[30] DOL CPP, Volume 10: Media Protection (MP), section 2.5, MP-12: Media Protection

After performing a root cause analysis, the OIG determined that conflicting media encryption policies between endpoint configuration managers allow the removed media to be unencrypted.

Improperly configured data loss prevention tools could lead to unauthorized sensitive data being removed from DOL and increasing the risk of data leakage, privacy incidents, and cybersecurity breaches.

We did not provide a new recommendation as the finding has already been remediated. We inspected evidence of newly configured policies and reperformed the failed test. Ultimately, a user was unable to move files to a USB device.

Finding 14: Data Exfiltration Testing

During the data exfiltration exercise, the following control deficiencies were identified:

- outbound emails containing PII were sent outside of the DOL networks,
- external AI-based platforms were used to process PII, and
- removable media was used to move data outside of the DOL networks.

According to the DOL CPP, DOL should monitor inbound and outbound communications traffic in near real time for enterprise or system-defined unusual or unauthorized activities or conditions.[31] Additionally, DOL should restrict the use of personal removable media on all systems and system components using technical and nontechnical controls.[32]

DOL has not defined policies regarding the use of publicly available AI platforms or implemented mature controls to block outbound traffic containing PII and to limit the use of removable media.

Without effective data exfiltration controls, DOL has increased vectors for unauthorized data exfiltration and increased risks for unauthorized release of sensitive Department data or PII.

We recommend the CIO:

9. Develop and implement effective data exfiltration controls to ensure unauthorized data does not leave the DOL network.

[31] DOL CPP, Volume 17: System and Information Integrity, section 2.4.4 SI-4(4): System Monitoring | Inbound and outbound Communications Traffic
[32] DOL CPP, Volume 10: Media Protection (MP), section 2.7 MP-7: Media Use

CONCLUSION

We reported 14 findings identified in 3 of the 6 FISMA Cybersecurity Functions (Govern, Identify, and Protect) and in 6 of the 10 FISMA Metric Domains (CG, C-SCRM, RAM, CM, IDAM, and DPP). As a result of our findings, we made nine recommendations to strengthen DOL's information security program. To improve the maturity of its information security program, DOL should consider applying these recommendations to its entire universe of systems.

Out of 16 previously open recommendations identified, we determined that 6 recommendations remained open and were not submitted for closure during FY 2025. Of the 10 open recommendations submitted for closure, we determined 2 should not be closed as the associated findings were again identified during the performance audit period and will remain open until other remediation efforts are completed. The remaining eight recommendations were successfully closed by DOL, and the issues did not reoccur during the performance audit period. DOL management should also implement a process to determine whether these recommendations apply to other information systems maintained in the organization's FISMA system inventory and address accordingly.

We assessed DOL's information security program as Consistently Implemented (Level 3), which was ineffective according to OMB's FY 2025 IG FISMA Reporting Metrics guidance.

The agency's response to the draft report is included in its entirety in Appendix F, and our analysis of the response can be found in Appendix E.

APPENDIX A: SCOPE, METHODOLOGY, AND CRITERIA

Scope

In accordance with FISMA, the objective of this performance audit was to determine to what extent DOL has implemented its information security program as established by the effectiveness of the relevant agency-wide and system-specific information system controls. As such, we assessed relevant security controls and processes referenced in the six Cybersecurity Framework Function areas outlined in the FY 2025 IG FISMA Reporting Metrics. We responded to the FY 2025 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of DOL OIG.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; Core Metrics and Supplemental Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memoranda referenced in the reporting metrics; and the DOL CPP. We assessed the DOL information security program at the program level, as well as the design and effectiveness of system-level policies and procedures for each information system selected for testing.

We made a judgmental[33] selection of 20 information systems (15 federal and 5 contractor information systems) from a total population of 63 information systems that comprised DOL's FISMA inventory as of January 1, 2025. We selected three general support systems due to their importance to IT infrastructure and mission criticality. The other systems were randomly selected. We determined an approximate distribution of the selected systems based on the number of systems managed by the IT Shared Services and owned by the respective agencies. We weighted our random selection based on certain factors, such as systems that are deemed "mission critical," cloud systems, systems that contain PII, systems that have never been tested before, systems that have not been tested within the last 2 years, and systems that contain financial information. Our testing also included DOL-wide information security controls.

Methodology

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

[33] Judgmental sampling is a non-probability sampling technique in which the sample members are chosen based on the auditor's knowledge and judgment.

conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by 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.

Sampling

To determine a control sample size, we considered the size of the population (i.e., the number of occurrences of the control) and other factors indicating risk of failure, including fraud risk, as described here:

- **Sample sizes where population > 5,000 items** – For control test work where the population size exceeded 5,000 items, we selected a sample of 45 items (assuming zero exceptions) per GAO's Financial Audit Manual (FAM) guidance to support the preliminary assessments of controls and conclude on the effectiveness of the controls.

- **Sample sizes where population < 5,000 items** – Per FAM guidance for populations containing less than or equal to 5,000 items (i.e., testing of daily, weekly, monthly, quarterly controls, or the size of the population), we used the minimum sample size (assuming zero exceptions), which is consistent with prior DOL FISMA performance audits (see Table 5).

Table 5 provides the frequency of control operation (population size) and the minimum sample size.

Table 5: Minimum Sample Size Based on Frequency of Control Operation (Population Size)

Frequency of Control Operation (Size of the Population)	Minimum Sample Size
Annual (1)	1
Quarterly (2–4)	2
Monthly (5–12)	2
Weekly (13–52)	5
Daily (53–365)	15
Recurring Manual (multiple times per day) (>365)	25

Source: GAO's FAM guidance

Approach to the Performance Audit

We agreed with DOL OIG on the following approach for conducting this performance audit and determining the maturity levels for each of the 6 Cybersecurity Framework Functions and 10 FISMA Metric Domains from the Core Metrics and Supplemental Metrics:

- For the Core Metrics and Supplemental Metrics, we requested DOL 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 DOL. 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.

- If we identified control deficiencies associated with prior year recommendations, we issued a "factual accuracy" finding draft to confirm the deficiency and noted it as a finding with no new recommendations.

- We performed test procedures over select security controls performed by management and in-scope systems (where applicable), leveraging Maturity Level 3 (Consistently Implemented) questions within the 10 FISMA Metric Domains. If we identified one or more 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 10 FISMA Metric Domains. If we identified one or more findings associated with metrics that were tested in consideration of Maturity Level 4 questions, we considered the nature of the identified finding(s) and assessed the maturity at Level 4 or 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 10 FISMA Metric Domains. We performed these procedures to evaluate the design of the metrics. If we identified one or more 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.

Based on the results of our test procedures, we input the maturity level for each of the Core Metrics and Supplemental Metrics into the CyberScope reporting

tool, which calculated the Cybersecurity Framework Function maturity levels based on the calculated average of the FISMA Metric Domain levels. The Core Metrics and Supplemental Metrics were averaged independently to determine a domain's maturity calculation. The calculated average scoring model was used for FY 2025. As part of this approach, Core Metrics and Supplemental Metrics were averaged independently to determine a domain's maturity calculation and to provide data points for the assessed program and function effectiveness. Within the context of the maturity model, OMB believes that achieving a Level 4 (Managed and Measurable) or above represents an effective level of security.

We performed the following procedures to assess the effectiveness of the information security program and practices of DOL:

- inquiry of information system owners, Information System Security Officers, system administrators, and other relevant individuals to walk through each control process;

- inspection of the information security policies and procedures established by OCIO and in use across DOL;

- observation of key controls within the information security program, control operators performing assigned duties, and tools used to perform cybersecurity related activities; and

- inspection of artifacts to determine the design, implementation, and operating effectiveness of security controls at the program and system levels.

We performed our fieldwork for the OIG FISMA Metric from December 14, 2024, through June 30, 2025, and fieldwork for the additional access controls testing was performed until October 1, 2025. All testing was performed through virtual meetings, walk-throughs, and observations with DOL representatives. Additionally, we held regular status meetings with DOL and OIG management.

Criteria

We considered federal information security guidance developed by NIST and OMB when developing and executing our FISMA performance audit approach. NIST Special Publications provide guidelines for use in the development and implementation of agencies' security programs. We used NIST Special Publication 800-53, Revision 5.1, Release 5.1.1, in our assessment of relevant information security controls. We also utilized DOL's CPP, which outlines DOL's requirements for information security. Finally, we utilized the FedRAMP Continuous Monitoring Review Standard Operating Procedure to evaluate DOL's controls supporting cloud service provider monitoring.

Data Exfiltration Testing

We performed data exfiltration testing over all networks within the Department; including the overall department's network, DOL OIG, BLS, and Job Corps networks to determine the operating effectiveness of data exfiltration and data lose prevention controls. We selected 20 test scenarios to perform. Fictitious PII was generated to attempt to remove data from the DOL networks through a variety of means. The tests cases were performed on each network by a data exfiltration specialist on the KPMG team.

Additional Access Control Testing

In addition to the testing procedures performed for the FY 2025 IG FISMA Metrics, we performed additional procedures to determine the effectiveness of access controls across 87 of 201 systems and subsystems at DOL—specifically, user access provisioning and deprovision across DOL applications, IT infrastructure, and supporting tools.

The following test procedures were performed:

- **Access Authorization Test Procedures:** We obtained user access listings for each application and information system and determined if access was provisioned in accordance with DOL policy.

- **Access Removal Test Procedures:** We obtained user access listings and Human Resources records for each application and information system and determined if access was deprovisioned in accordance with DOL policy.

APPENDIX B: FINDING REFERENCE

Finding No.	Function	Domain	Issued Finding
1	Govern	Cybersecurity Governance	FISMA-25-11
2	Govern	Cybersecurity Governance	FISMA-25-15
3	Govern	Cybersecurity Supply Chain Management	FISMA-25-10
4	Identify	Risk and Asset Management	FISMA-25-01 FISMA-25-07
5	Identify	Risk and Asset Management	FISMA-25-09
6	Identify	Risk and Asset Management	FISMA-25-13
7	Protect	Configuration Management	FISMA-25-16
8	Protect	Identity and Access Management	FISMA-25-02 FISMA-25-03 FISMA-25-05 FISMA-25-06
9	Protect	Identity and Access Management	FISMA-25-04
10	Protect	Identity and Access Management	FISMA-25-14
11	Protect	Identity and Access Management	FISMA-25-22 FISMA-25-23 FISMA-25-24
12	Protect	Identity and Access Management	FISMA-25-25
13	Protect	Data Protection and Privacy	FISMA-25-08
14	Protect	Data Protection and Privacy	FISMA-25-18 FISMA-25-19 FISMA-25-21

APPENDIX C: STATUS OF PRIOR YEAR RECOMMENDATIONS

As part of the FY 2025 FISMA performance audit, we followed up on the status of management's corrective actions to remediate prior year findings. We evaluated the corrective actions to determine whether the recommendations were implemented and whether the conditions and causes were addressed by management. If there was evidence that a recommendation had been sufficiently implemented and there were no related issues identified during our FY 2025 testing, we determined the recommendation was closed. If there was evidence a recommendation had been only partially implemented or not implemented at all, we determined the recommendations remained open. At the beginning of FY 2025, we determined there were 16 open prior year FISMA recommendations. Based on our testing, we determined eight recommendations were closed and eight recommendations remained open (see Table 6).

Table 6: Progress DOL Has Made in Closing Prior Year Recommendations

Related Domain	Report Year	Prior Year Recommendation	Status of Recommendation
C-SCRM	2024	Develop and implement an unambiguous standard operating procedure, utilizing Federal Risk and Authorization Management Program guidance and leading practices, to monitor cloud service providers and escalate noncompliance effectively to the agency Authorizing Official, including defined risk management deficiency triggers.	Open
RAM	2015	We recommend the Assistant Secretary of the Office of Administration and Management realign the organizational structure as it relates to the CIO to address the organizational independence issue identified in this report.	Open

RAM	2022	Update DOL entity-wide and system-level security policies, procedures, and plans to comply with NIST SP 800-53, Rev. 5.	Open
CM	2019	Develop and implement performance metrics for configuration management.	Closed
CM	2020	Implement a process for approving deviations from established configuration settings.	Closed
CM	2021	Enforce DOL requirements for implementing, auditing, testing and documenting exceptions to baseline configurations.	Closed
IDAM	2019	Finalize the implementation of the access control technologies.	Closed
IDAM	2024	Develop and implement a validation of the provisioned exemptions to ensure all provisioned exemptions are provisioned appropriately.	Closed
IDAM	2024	Complete in progress efforts to modernize impacted systems and subsequently enable multi-factor authentication.	Open
IDAM	2024	Enhance the validation process for the quarterly Chief Information Officer FISMA Metrics to ensure all metrics are reported accurately and are in accordance with applicable guidance and standards.	Open
IDAM	2024	Assign appropriate resources to perform the audit log reviews as required by the system security plan.	Closed

DPP	2019	Implement data encryption configurations/solutions at the server level for data at rest for sensitive information (PII).	Closed
DPP	2022	Implement data loss prevention tools and alerts based on the results of agencies' data exfiltration tests.	Open
DPP	2024	Develop, implement, and track privacy-focused, role-based training for employees and contractors with significant privacy responsibilities.	Open
ST	2024	Develop and implement validation controls to ensure users are properly onboarded to LearningLink and assigned required trainings.	Closed
ISCM	2021	Develop clear standards for the documentation of information security controls and enforce the adherence to these standards through OCIO monitoring processes for developing, reviewing and maintaining system security plans and documentation.	Open

APPENDIX D: ACRONYMS AND ABBREVIATIONS

Acronym / Abbreviation	Definition
AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
BLS	Bureau of Labor Statistics
CG	Cybersecurity Governance
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
CPP	Cybersecurity Policy Portfolio
CSAM	Cybersecurity Assessment Management
C-SCRM	Cybersecurity Supply Chain Risk Management
Department or DOL	U.S. Department of Labor
DHS	U.S. Department of Homeland Security
DPP	Data Protection and Privacy
FAM	Financial Audit Manual
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
IDAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

Acronym / Abbreviation	Definition
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identification Verification
RAM	Risk and Asset Management
SCRM	Supply Chain Risk Management
ST	Security Training
USB	Universal Serial Bus

APPENDIX E: KPMG'S ANALYSIS OF THE AGENCY'S RESPONSE TO THE REPORT

OCIO generally concurred with all of KPMG's recommendations in the FY 2025 DOL FISMA Report. In management's response, OCIO reinforced management's commitment to cybersecurity and the ongoing updates to improve DOL's IT cybersecurity portfolio. OCIO will provide corrective action plans—which will address and close the recommendations upon implementation—to the OIG for its consideration.

APPENDIX F: AGENCY'S RESPONSE TO THE REPORT

The agency's response to the draft report follows.

U.S. Department of Labor

Office of the Assistant Secretary for Administration and Management
Washington, D.C. 20210

MEMORANDUM FOR: LAURA B. NICOLOSI
Assistant Inspector General for Audit

FROM: MANGALA KUPPA
Chief Information Officer

MANGALA KUPPA Digitally signed by MANGALA KUPPA Date: 2026.04.16 16:48:23 -04'00'

SUBJECT: Management Response to DRAFT REPORT – (Fiscal Year) FY 2025 FISMA DOL Information Security Report, 23-26-001-07-725

This memorandum responds to the Draft Report – FY 2025 FISMA DOL Information Security Report (23-26-001-07-725), issued on April 6, 2026, for departmental review. Information security remains one of the Department's highest priorities, and DOL leadership is committed to continually advancing the maturity, resilience, and operational effectiveness of the Department's cybersecurity program. DOL management appreciates the extensive work performed by the independent auditors and values the insights provided to strengthen our risk management, governance, and defensive cyber capabilities.

Management concurs with the current-year findings identified during the FY 2025 FISMA audit evaluation. In each case, corrective actions are either already completed, underway, or formally planned. The Department looks forward to engaging the Office of Inspector General (OIG) to achieve timely resolution and closure of these recommendations.

Although the FY 2025 audit determined that DOL's information security program remains below the *effective* threshold, the Department affirms that significant progress has been made. We continue to demonstrate quantifiable maturity gains and strengthened internal controls across the cybersecurity framework functions. Our FY 2025 advancements reflect ongoing, meaningful improvements to governance, identity and access management, secure configuration, data protection, and continuous monitoring.

In Fiscal Year 2025, we continued to enhance the Department's Cybersecurity and Privacy Program, with a focused emphasis on capabilities prioritized in Executive Order (EO) 14306, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity*, and amendments to EO 13694 and EO 14144. Our efforts reflect a sustained commitment to strengthening DOL's defenses, modernizing enterprise capabilities, and maturing our risk-informed cybersecurity posture. DOL accomplished the following activities during FY 2025:

- **Expanded Zero Trust Adoption:** We made significant progress implementing enterprise-wide solutions that advance zero trust principles, including broader enforcement of multifactor authentication and increased deployment of encryption for data-at-rest and in-transit.
- **Enhanced Continuous Monitoring and Automation:** We increased automation within our Information Security Continuous Monitoring (ISCM) program, improving the accuracy, timeliness, and actionability of risk insights across DOL agencies. These improvements strengthen our ability to rapidly detect, assess, and respond to potential threats.
- **Strengthened Identity, Credentialing and Access Management (ICAM):** The Department expanded PIV-based authentication, matured privileged access management through CyberArk, and strengthened account provisioning controls. These advancements further reduce unauthorized access risks and support compliance with federal identity mandates.

- **Improved CSAM Data Integrity and Governance:** We improved enterprise visibility and risk management by enhancing the Cybersecurity Assessment and Management (CSAM) tool's data quality—correcting system inventories, updating system ownership records, and validating interconnection documentation.
- **Advanced Supply Chain and Cloud Security:** We improved oversight of cloud service providers by implementing additional FedRAMP monitoring checkpoints, documenting risk exceptions more rigorously, and strengthening continuous monitoring of third-party environments.
- **Expanded Data Protection and Privacy Safeguards:** The Department strengthened data loss prevention (DLP) capabilities, improved email scanning controls, and implemented new guardrails around unauthorized use of generative AI platforms to reduce the risk of inadvertent data exposure.
- **Continuous Threat Monitoring and Vulnerability Reduction:** DOL maintained 24x7 threat detection and response capabilities, providing continuous vigilance that minimized operational risk. We collaborated with the Cybersecurity and Infrastructure Security Agency (CISA) on penetration testing and adopted additional continuous monitoring mechanisms that identified previously unknown vulnerabilities. The Department continued participation in CISA's Vulnerability Disclosure Policy (VDP) platform to support responsible reporting and remediation of externally identified vulnerabilities.
- **Strengthened cybersecurity posture through responsible Artificial Intelligence (AI) Adoption:** Integrated AI enabled automation and analytics into core cybersecurity processes—enhancing continuous monitoring and reducing manual workloads, while fully aligning with DOL's Responsible AI policy requirements, including adherence to privacy safeguards and the Department's cybersecurity program to ensure the confidentiality, integrity, and availability of all AI systems.
- **Enhanced SOC reporting efficiency through automation:** Implemented new processes that significantly reduce the time required to compile Security Operations Center (SOC) reports, accelerating the generation of vulnerability management reports.
- **Resolution of Prior-Year Findings:** We successfully closed eight prior-year audit recommendations and advanced several others toward completion, reinforcing our commitment to continuous improvement and reduction of legacy risks.

These accomplishments illustrate DOL's continued momentum and demonstrate our strong commitment to protecting agency systems, personnel, and data.

Looking ahead, DOL will continue to focus on strengthening program maturity in FY 2026, prioritizing the following areas:

- Completing implementation of MFA across all systems and modernizing authentication mechanisms for legacy platforms.
- Enhancing DOL's enterprise log management and detection capabilities in alignment with OMB M-21-31.
- Advancing zero-trust maturity, with expanded micro segmentation, improved identity governance, and strengthened endpoint defenses.
- Improving governance and accountability structures to ensure clarity of roles and responsibilities across all DOL agencies.
- Expanding the use of automation and analytics to accelerate vulnerability identification, incident response, configuration compliance, and information system authorizations.
- Finalizing and implementing DLP controls to prevent data exfiltration and strengthen agency protections for sensitive information.
- Continuing progress toward quantum-resistant cryptography and adoption of secure next-generation networking capabilities.

- Improving policy alignment and operational readiness for the responsible adoption of AI/ML technologies across the Department.

As demonstrated in the draft FISMA report, DOL has built a strong foundation for an effective cybersecurity program and will continue to improve operational rigor consistent with OIG recommendations. Cybersecurity is a continuous journey, and DOL remains committed to operating a secure, resilient, and modernized information security program.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202) 693-4242 or have your staff contact Muhammad Butt, Senior Advisor for Cybersecurity Initiatives and Acting Chief Information Security Officer (CISO) at (202) 693-1000 (extension 16615) or Butt.Muhammad@dol.gov. As the acting CISO, Muhammad Butt is responsible for the corrective actions identified in this correspondence.

cc: Dean Heyl, Assistant Secretary for Administration and Management
Braye Cloud, Deputy Assistant Secretary for Operations
Muhammad Butt, Senior Advisor for Cybersecurity Initiatives and Acting Chief Information Security Officer (CISO)
Gary McCoy, Acting Division Chief for Cybersecurity Governance

3

REPORT FRAUD, WASTE, OR ABUSE TO THE DEPARTMENT OF LABOR

Online
https://www.oig.dol.gov/hotline.htm

Telephone
(800) 347-3756 or (202) 693-6999

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue NW
Room S-5506
Washington, DC 20210