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

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2024 FISMA DOL INFORMATION SECURITY REPORT: CONTINUED IMPROVEMENT OF INFORMATION SYSTEM 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.

Carolyn R. Hantz

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

DATE ISSUED: DECEMBER 10, 2024
REPORT NUMBER: 23-25-002-07-725

BRIEFLY...

FY 2024 FISMA DOL INFORMATION SECURITY REPORT: CONTINUED IMPROVEMENT OF INFORMATION SYSTEM 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 the Department'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 also 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) 2024 information security program for the period October 1, 2023, through June 30, 2024. 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 and improve; however, certain Cybersecurity Framework Functions are preventing DOL from maintaining an effective information security program. KPMG reported eight findings for DOL's information security program. The findings were identified in two of five FISMA Cybersecurity Framework Functions and in four of the nine 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 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 five FISMA Cybersecurity Framework Functions: Identify, Protect, and Recover. Specifically, KPMG identified deficiencies in the monitoring of DOL cloud service providers, multi-factor authentication enforcement, security training compliance, and the implementation of privacy-focused role-based training.

In addition, 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 (NIST) standards and guidelines. For example, DOL's system-level security policies have not been updated to comply with NIST Special Publication 800-53, Revision 5.1, Release 5.1.1, Security and Privacy Controls for Information System and Organization. The OIG remains concerned that this prior year finding of compliance with the NIST publication remains outstanding. By not updating DOL's policies and procedures to be compliant, the Chief Information Officer is not taking necessary steps in mitigating IT risk for DOL.

WHAT WE RECOMMENDED

KPMG made seven new recommendations to strengthen DOL's information security program. KPMG also determined 10 prior year recommendations were closed, 2 remain open, and 7 were not submitted for closure. DOL management generally concurred with the findings and recommendations; however, management disagreed with KPMG's conclusion that DOL's information security program was ineffective

READ THE FULL REPORT

For more information, go to: https://www.oig.dol.gov/public/reports/oa/2025/23-25-002-07-725.pdf.

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

Louis Charlier
Acting Chief Information Officer
U.S. Department of Labor
200 Constitution Avenue NW
Washington, DC 20210

The U.S. Department of Labor (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) 2024 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 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, 2023, through June 30, 2024. 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 eight findings for DOL's information security program. The findings were identified in two of five FISMA Cybersecurity Framework Functions and in four of the nine 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 2024 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 five FISMA Cybersecurity Framework Functions: Identify, Protect, and Recover.

In determining DOL's FY 2024 Assessed Maturity level for each function, the OIG and KPMG performed a risk-based analysis leveraging the auditors' knowledge and the FY 2024 Core Metrics results with the supplemental metric results for FY 2023 and FY 2024. The OIG and KPMG were not provided any additional information during the audit or afterwards to change this assessment.

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 (NIST) standards and guidelines. For example, DOL's system-level security policies have not been updated to comply with NIST Special Publication (SP) 800-53, Revision (Rev.) 5.1, Release (Rel.) 5.1.1, Security and Privacy Controls for Information System and Organization (NIST SP 800-53, Rev. 5, Rel. 5.1.1). KPMG noted further deficiencies in the monitoring of DOL cloud service providers, multi-factor authentication enforcement, security training compliance, and the implementation of privacy-focused role-based training.

KPMG made seven recommendations related to control deficiencies. KPMG did not make recommendations for one control deficiency because it corresponded to an open prior year recommendation. After evaluating the implementation of recommendations from prior FISMA reports, KPMG determined 10 recommendations were closed, 2 remained open, and 7 were not submitted for closure.

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

We remain concerned that the prior year finding regarding DOL's compliance with NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, remains outstanding. By not updating DOL's procedures to be compliant, the Chief Information Officer is not taking necessary steps in mitigating IT risk for the Department. We have also identified an example of this issue in another OIG audit. At the time of our 2024 audit of DOL's Wireless Network Security,[2] we determined that, because the System Security Plans were written for NIST SP 800-53 Rev. 4, instead of Rev. 5 as required, gaps existed in security policies and configuration settings, specifically in securing DOL wireless capabilities.

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

Carolyn R. Hantz
Assistant Inspector General for Audit

[2] DOL Implemented Its Wireless Network Securely, Though Security Gaps Exist in Testing, Updating, Patching, and Continuous Review, Report No. 23-24-003-07-720 (September 11, 2024)

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 2024

Acting 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 (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, 2023, through June 30, 2024.

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

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objective of this performance audit was to determine to what extent has 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 five Cybersecurity Function areas outlined in the Fiscal Year (FY) 2024 Inspector General (IG) FISMA Metrics, which included Core Metrics and Supplemental

Metrics Group 2.[3] We responded to the Core Metrics and Supplemental Metrics Group 2 and assessed the maturity levels on behalf of the DOL OIG. We also followed up on the status of prior year recommendations.

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 2024, a calculated average scoring model was used, and the Core Metrics and Supplemental Metrics Group 2 were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. Table 1 depicts DOL's assessed maturity levels for the five Cybersecurity Framework Functions in FY 2024.

Table 1: Maturity Levels for Cybersecurity Framework Functions

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

Source: FY 2024 Inspector General Section Report for DOL

During FY 2024, we tested security controls at the entity level and for a selection of 20 systems for each of the Cybersecurity Framework Functions. We identified eight findings for DOL's information security program. The findings were identified in two of the five FISMA Cybersecurity Framework Functions and in four of the nine FISMA Metric Domains. We considered the identified findings and five relevant open prior year recommendations when we assessed the maturity levels for each of the Core Metrics and Supplemental Metrics Group 2, which were input into the CyberScope reporting tool. Based on the calculated score from CyberScope and OMB guidance, DOL's information security program was determined to be "not effective."

[3] These metrics were provided in the Office of Management and Budget's guidance: FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics.

In addition to testing security controls, we evaluated the implementation of recommendations from prior information technology (IT) reports from 2019 through 2023. The IT reports included those prepared in connection with previous FISMA performance audits. Out of 19 previously open recommendations, we determined DOL successfully closed 10.

As reported in FY 2022 and FY 2023, DOL's system-level security plans and procedures still have not been updated to comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5.1, Release (Rel.) 5.1.1, Security and Privacy Controls for Information System and Organization (NIST SP 800-53, Rev. 5.1, Rel. 5.1.1). We noted further deficiencies in the monitoring of DOL cloud service providers (CSP), multi-factor authentication (MFA) enforcement, security training compliance, and the implementation of privacy-focused role-based training.

In response to these control deficiencies, we made seven recommendations related to strengthening DOL's information security program. We did not make recommendations for one control deficiency as it corresponded to an open prior year recommendation and was previously identified by management and tracked through a plan of action and milestones (POA&M). 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.

In its response to a draft of this report, DOL management expressed that it generally concurred with the findings and recommendations in the report but did not agree with the overall conclusion. As such, we included an additional response in Appendix B. DOL management's full response is included in Appendix C.

This report is intended solely for the use of DOL, DOL OIG, the U.S. Department of Homeland Security (DHS), the Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

December 4, 2024

BACKGROUND

We performed the FY 2024 FISMA performance audit under contract with DOL[4] as a performance audit in accordance with GAGAS. DOL OIG monitored our work to assess whether we met professional standards and contractual requirements.

Agency Overview

The mission of DOL is to foster, promote, and develop the welfare of the wage earners, job seekers, and retirees in the United States; improve working conditions; advance opportunities for profitable employment; and assure work-related benefits and rights. That mission includes administering and enforcing more than 180 federal laws. These mandates and the regulations that implement them cover workplace activities for about 10 million workplaces and 150 million workers.

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

The Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, DHS, the Federal Chief Information Officers council, and the Chief Information Security Officers Council, developed the Core Metrics and Supplemental Metrics Group 2[5] based on the five Cybersecurity Framework

[4] DOL Contract Number: 1604DC-20-A-0014
[5] OMB, FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, issued February 10, 2023, available at: https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf

Functions outlined in the NIST's Framework for Improving Critical Infrastructure Cybersecurity[6] (herein referred to as the Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.[7]

The Core Metrics and Supplemental Metrics Group were chosen based on alignment with Executive Order 14028 (specifically the multi-factor authentication and encryption section and the software supply chain security and critical software section),[8] as well as the following OMB guidance provided to agencies to further modernize federal cybersecurity:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09),[9]
- Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31),[10] and
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01).[11]

[6] NIST created "Functions" to organize basic cybersecurity activities at their highest level. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management.
[7] Executive Order 13636 calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and leading practices to help organizations manage cybersecurity risks. The resulting framework, created through collaboration between the government and the private sector, uses a common language to address and cost-effectively manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses. See Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued on February 12, 2013, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[8] Executive Order 14028, Improving the Nation's Cybersecurity, issued May 12, 2021, available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[9] OMB, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, M-22-09 (January 26, 2022), available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[10] OMB, Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents, M-21-31 (August 27, 2021), available at: https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf
[11] OMB, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response, M-22-01 (October 8, 2021), available at: https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf

In addition, OMB Memorandum M-23-03[12] adjusted the timeline for the IG evaluation. Specifically, OMB Memorandum M-23-03 required that a core group of metrics be evaluated annually and the remainder of the metrics be evaluated on a two-year cycle—as agreed to by CIGIE, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency. The rotating 2-year cycle metrics are denoted as the "Supplemental Metrics Group 1 (FY 2023)" and "Supplemental Metrics Group 2 (FY 2024)." Specifically, Core Metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness. Supplemental Metrics are assessed at least once every 2 years, represent important activities conducted by information security programs, and contribute to the overall evaluation and determination of information security program effectiveness.

The Core Metrics and Supplemental Metrics Group 2 use a capability maturity model developed by OMB, DHS, CIGIE, and other stakeholders for the nine FISMA Metric Domains. Table 2 outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domain.

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

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	Risk Management (RM) Supply Chain Risk Management (SCRM)
Protect	Configuration Management (CM) Identity and Access Management (IAM) Data Protection and Privacy (DPP) Security Training (ST)
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)
Recover	Contingency Planning (CP)

Source: FY 2023–2024 Inspector General FISMA Reporting Metrics

[12] OMB, Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements, M-23-03 (December 2, 2022), available at: https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf

IG FISMA Scoring

The ratings in the nine FISMA Metric Domains (RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a calculated average. The final scores were based on the calculated averages of assessed maturity levels based on the aforementioned capability model, as well as qualitative and quantitative measures used to make risk-based determinations of the overall security program.[13] When responses are entered into the CyberScope reporting tool, it automatically calculated the average of the Core Metrics and Supplemental Metrics Group 2 for each FISMA Metric Domain and Cybersecurity Framework Function. The capability model has five levels:

- Ad Hoc (Level 1)
- Defined (Level 2)
- Consistently Implemented (Level 3)
- Managed and Measurable (Level 4)
- Optimized (Level 5)

Table 3 details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework Function. According to the FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, OMB believes that achieving a Level 4 (Managed and Measurable) rating or above represents an effective level of security. For FY 2024, a calculated average scoring model was used, and the Core Metrics and Supplemental Metrics Group 2 were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness.

[13] 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 2023–2024 Inspector General FISMA Reporting Metrics

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.

RESULTS

Based on the ratings for each 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. A security program is considered effective if the calculated average of the Core Metrics and Supplemental Metrics Group 2 are at least Managed and Measurable (Level 4).

Table 4 depicts the maturity levels determined for the five Cybersecurity Framework Functions and their corresponding FISMA Metric Domains.

Table 4: FY 2024 Cybersecurity Framework Function Maturity Levels

Cybersecurity Framework Functions	Maturity Level
Identify – RM and SCRM	Consistently Implemented (Level 3)
Protect – CM, IAM, DPP, and ST	Consistently Implemented (Level 3)
Detect – ISCM	Managed and Measurable (Level 4)
Respond – IR	Managed and Measurable (Level 4)
Recover – CP	Consistently Implemented (Level 3)

Source: FY 2024 DOL CyberScope Response

DOL continued to make improvements to its information system security program, specifically in areas related to ISCM and vulnerability management. DOL developed tiered reports that give visibility to information system risks at various levels and provide quantitative and qualitative performance measures on the effectiveness of the ISCM program. Additionally, DOL enhanced its vulnerability remediation process to help ensure critical and high vulnerabilities are remediated timely and prioritized vulnerability remediation is based on risk. DOL closed multiple prior year recommendations to enhance its vulnerability management program.

We have also identified areas of improvement that would enable DOL to reach a Managed and Measurable rating which, according to OMB, is reflective of an effective information security program. For example, DOL has made continued improvements within the CM function area; however, a gap remains in its use of configuration and common secure settings on its information systems. DOL currently has three open prior year recommendations related to approving deviations from established configuration settings, developing and implementing performance metrics for configuration management, and documenting exceptions to baseline configurations.

In the CP function area, DOL should monitor both qualitative and quantitative performance measures of system backup and storage. It also needs to ensure that alternate storage and processing sites are configured to support recovery operations as part of its continuous monitoring program. DOL should also employ automated mechanisms to effectively test information system contingency plans.

Additionally, we determined DOL did not require specific privacy role-based training for employees or contractors with significant privacy responsibilities. However, DOL has established a dedicated Privacy Office to handle all items related to privacy including trainings. The Privacy Office performed a self-assessment of DOL's capabilities and plans to create specific training for employees and contractors with significant privacy responsibilities.

Finally, DOL lacks performance metrics relating to the SCRM function area. To achieve a Managed and Measurable maturity level within this function area, DOL should implement qualitative and quantitative performance measures to monitor and report on the effectiveness of SCRM policies and procedures and DOL-defined products, systems, and services provided by external providers.

We also evaluated the implementation of recommendations from prior IT reports from 2019 through 2023. The IT reports included those prepared in connection with previous FISMA performance audits. Out of 19 previously open recommendations, we determined DOL successfully closed 10 recommendations.

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 RM decisions.

We assessed OCIO's Identify function as Consistently Implemented (Level 3). As described in detail below, OCIO did not update system-level policies and procedures to be compliant with NIST SP 800-53, Rev. 5.1, Rel. 5.1.1; however, OCIO continued to make updates through a phased approach in-line with the Annual Security Control Assessment process. Additionally, OCIO's monthly continuous monitoring of CSPs was ineffective.

Risk Management

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. RM 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 RM 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 RM FISMA Metric Domain as Managed and Measurable (Level 4). OCIO implemented policies and procedures to maintain a complete and accurate inventory of its major information systems, hardware devices, and software. 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 performed the risk-based allocation of resources based on system categorization, including for the protection of high-value assets, as appropriate, through collaboration and data-driven prioritization.

OCIO used the Cybersecurity Assessment Management 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 Register, which included system POA&Ms and risk responses. The Cybersecurity Risk Register 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 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 all its information systems according to their priority in enabling the agency mission and business functions. The prioritization was performed through a risk-based allocation of resources based on system categorization. OCIO implemented an Asset Value Scoring system to calculate scores for each information system by aggregating information stored in the Cybersecurity Assessment Management tool and to identify high value assets for DOL to meet its mission essential functions.

Additionally, OCIO developed an information security architecture to provide a structured methodology for managing risk. OCIO implemented automated tools to maintain a broad view of its enterprise and has an Enterprise Architecture Strategic Roadmap to guide future development. However, OCIO did not develop a process to validate that its security engineering and system life cycle processes were effectively implemented across DOL.

As a part of the transition to the NIST SP 800-53 Rev. 5.1, Rel. 5.1.1, OCIO has implemented the DOL Cybersecurity Policy Portfolio (CPP) at the department

level. Previously, in FY 2022, we recommended[14] OCIO update the entity-wide and system-level security procedures and plans to comply with NIST SP 800-53, Rev. 5.1, Rel. 5.1.1. In response to our finding and recommendation, OCIO created a POA&M to track the deficiency and execution of a plan to update system-level policies and procedures in conjunction with their Annual Security Control Assessments. One third of the controls are rotated and tested annually as a part of these assessments. OCIO informed us that the controls will be updated to NIST SP 800-53, Rev. 5.1, Rel. 5.1.1, once tested in the assessment. Until this 3-year cycle is complete, each system security plan will not comply with NIST SP 800-53, Rev. 5.1, Rel. 5.1.1.

Supply Chain Risk Management

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. We tested the third-party annual assessments for five contractor systems and determined they were conducted in accordance with the CPP.

Based on the results of our performance audit procedures, we assessed DOL's SCRM FISMA Metric Domain as Consistently Implemented (Level 3). OCIO developed and implemented SCRM standards and procedures to assess supply chain risks associated with suppliers and contractors and to help ensure that counterfeit components are detected and prevented from entering DOL systems.

OCIO performed annual assessments of CSPs to assess whether controls of systems or services provided by contractors complied with FISMA requirements; however, the monthly continuous monitoring program for CSPs was ineffective because control operators did not follow defined procedures to identify and follow up on deficient deliverables. Additionally, OCIO did not develop and implement qualitative and quantitative performance measures to gauge the effectiveness of its information security performance related to SCRM.

[14] FY 2022 FISMA DOL Information Security Report: DOL's Information Security Program Not Remaining Current with Security Requirements, Report No. 23-23-001-07-725 (February 10, 2023), available at: https://www.oig.dol.gov/public/reports/oa/2023/23-23-001-07-725.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 Consistently Implemented (Level 3). While DOL implemented procedures and policies for CM, IAM, DPP, and ST, our testing found deficiencies associated with the implementation and effectiveness of controls in the IAM, DPP, and ST 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). While we noted OCIO developed and implemented CM policies and procedures, we found deficiencies—related to prior year recommendations—associated with the baseline configuration deviation process. OCIO implemented and communicated an enterprise-wide configuration management plan, which defines roles and responsibilities of configuration management stakeholders. The configuration management 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.

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, OCIO did not close a prior year recommendation to develop a process to approve deviations from established configuration settings and document exceptions to baseline configurations.

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 IAM Domain includes the requirement that an agency must implement a set of capabilities to help ensure users authenticate IT resources and only have access to resources that are required for their job function—a concept referred to as "need to know." The supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges. These activities collectively are referred to as Identity, Credential, and Access Management.

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

OCIO implemented a department-wide process for assigning position designations and performing screening prior to granting access to information systems. All DOL positions were assigned a designation, and the appropriate security screening procedures were performed before a potential DOL employee or contractor was onboarded. DOL implemented automated tools to manage and track this process.

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. For 1 of the 25 users selected for testing who utilize a Personal Identification Verification (PIV) Card exemption, the proper documentation was not gathered, and the established procedure for PIV exemptions was not followed. Additionally, two systems were not configured to require MFA for non-privileged users. Finally, OCIO misreported the number of systems that complied with Executive Order 14028 MFA requirements in its quarterly Chief Information Officer (CIO) FISMA Metrics.

OCIO made progress toward automating privileged account management by enhancing its tools and capabilities. For example, at the time our audit, OCIO was implementing, in a phased approach, a tool to support the automation of privileged account management. Specifically, OCIO had begun the deployment of privileged account management tools; however, the automated solution was not deployed across DOL. For one selected system, management did not perform a periodic review of audit log activity. Additionally, for one selected

system, the information that was used as the basis of the periodic review of privileged users was not reliable or relevant.

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,[15] 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[16] 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). In accordance with Executive Order 13719, OCIO appointed a Senior Agency Official for Privacy, who has overall responsibility for establishing and overseeing the Privacy Program at DOL. As of October 1, 2024, OCIO established a separate Privacy Office, outside of the Cybersecurity Directorate, to oversee and maintain all governance related to privacy. However, like the previous year, OCIO did not sufficiently encrypt data-at-rest at the server level, despite making progress on this issue. In accordance with Executive Order 14028, and as of April 19, 2024, OCIO reported 86 percent of FISMA-reportable systems implemented encryption of data-at-rest.[17]

---

[15] 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

[16] Executive Order 13719, Establishment of the Federal Privacy Council, issued February 9, 2016, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council

[17] The percentage was reported as a part of the FY 2024 Q2 CIO FISMA Metrics. These metrics are a quarterly submission to OMB to monitor agencies' progress towards the implementation of cybersecurity priorities. For more information, see FY 2024 CIO FISMA Metrics, Version 1.0 (December 2023), available at: https://www.cisa.gov/sites/default/files/2023-12/FY24_FISMA_CIO_Metrics_v1.0_FINAL_1.pdf.

OCIO implemented controls to prevent data extraction and enhanced network defenses through tools that utilized website filtering policies, email data loss prevention tools, outbound network traffic monitoring, and the blocking of known malicious domains and indicators of compromise. Additionally, OCIO implemented a data breach plan designed to work in conjunction with the newly formed Privacy Office, Department of Labor Computer Security Incident Response Center, and United States Computer Emergency Readiness Team as needed.

Finally, OCIO implemented privacy-focused security training that all users must complete prior to gaining access to any DOL system; however, OCIO did not implement privacy-focused role-based training for users with responsibilities for handling and safeguarding PII. DOL's Privacy Office has been tasked with the governance and management of all privacy related matters at DOL to include privacy-focused role-based training.

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 its message.

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. However, OCIO failed to ensure that all users completed their annual security awareness training, as 1 of the 25 users selected for testing did not complete the training.

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

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 all 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 implemented the functionality to utilize the system security-related information to enable the effective operation of its systems under Ongoing Authorization 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 DHS and utilized DHS tools 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 United States Computer Emergency Readiness Team guidelines. Additionally, OCIO captured the impact of incidents and used the information 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. 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, 13 of 15 DOL information systems selected for testing performed manual tabletop CP exercises, in lieu of functional or automated CP tests.

AUDIT FINDINGS AND RECOMMENDATIONS

DOL's information security program continues to mature and improve; however, certain Cybersecurity Framework Functions are preventing DOL from maintaining an effective information security program. As a result of our work, we identified eight findings and made seven new recommendations. OCIO's continuous improvements, including addressing open prior year recommendations, and its implementation of new technologies will make its program more effective and enable its growth to higher maturity levels.

Identify – Supply Chain Risk Management

Finding 1: Improperly Designed Cloud Service Provider Continuous Monitoring

DOL did not follow Federal Risk and Authorization Management Program's (FedRAMP) leading practices for monitoring CSPs. OCIO management failed to consistently verify that CSPs completed their FedRAMP continuous monitoring requirements. Additionally, DOL did not consistently follow its internal FedRAMP

Continuous Monitoring Review Standard Operating Procedures (SOP). We also noted that, when a CSP missed more than two consecutive months of continuous monitoring reports, OCIO did not document these instances in its review and could not provide evidence that they were escalated to the authorizing official.

The FedRAMP Continuous Monitoring Performance Management Guide[18] (the Management Guide) specifies the guidance and leading practices for monitoring CSPs. This guidance states that each agency that issues an Authorization to Operate to a CSP must review the CSP's continuous monitoring activities to assess whether the CSP is effectively performing its security controls according to the agency's risk tolerance. These monitoring activities include, but are not limited to, the review of monthly POA&M and vulnerability reports, and the performance of annual assessments. Additionally, the Management Guide outlines a structured and formal escalation process that agencies should implement to monitor their authorized CSPs.

OCIO developed and implemented a FedRAMP Continuous Monitoring Review SOP to document how its reviewers should perform and document their continuous monitoring review. The SOP requires that the reviewer verify each relevant artifact. If issues are noted, the reviewer should reach out to the CSP for clarity.

OCIO did not consistently verify that CSPs completed their continuous monitoring requirements because DOL personnel did not follow the internal SOP for monitoring third party CSPs. The internal SOP was vague and did not provide the control operator with clear instructions for review practices.

The lack of a properly designed continuous monitoring process for CSPs can lead to vulnerabilities on cloud systems going unnoticed or unremedied, which increases risks to the confidentiality, availability, and integrity of DOL data.

We recommend the CIO:

1. 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 non-compliance effectively to the agency Authorizing Official, including defined risk management deficiency triggers.

[18] FedRAMP Continuous Monitoring Performance Management Guide, Version 3.0 (August 30, 2023)

Protect – Identity and Access Management

Finding 2: Undocumented PIV Exemption

During our testing of 15 devices, we found 1 device did not have an associated Enterprise Service Desk (ESD)-18 form documented for the 365-day PIV exemption provisioned. OCIO was unaware that an administrative user was granted a 365-day PIV exemption without the proper documentation and approval. Specifically, an administrator granted his own 365-day PIV exemption without completing the required ESD-18 for his exemption, as required by the PIV Exemption SOP.

The ESD-18 form is an administrator request form that all infrastructure administrators must complete prior to a PIV exemption being provisioned. The ESD-18 form documents the administrator, the machine to be added to the PIV exemption group, the duration of the exemption, and management approval. Furthermore, the Admin PIV Exemption Standard Operating Procedures states, "IT Admins are required to have a signed ESD-18 form to receive 365-day PIV Exemption. No exceptions."

OCIO informed us that the deficiency occurred because responsible personnel did not consistently validate whether all exemptions were provisioned in accordance with the exemption SOP. The ESD-18 form was not completed prior to provisioning the PIV exemption for the selected device. The device was assigned to an administrator; thus, the administrator was able to provision the exemption for his own device without prior documented approval. OCIO management informed us that the administrator who provisioned the exemption was aware of the established procedure; however, he knowingly did not follow the procedure and was unable to justify the noncompliance with a reasonable explanation. The administrator has since been retrained on the proper procedures.

The failure to document exceptions to the PIV requirement and the provisioning of exemptions for a person's own devices could result in unauthorized access to confidential information or unauthorized changes made to a system that could impact the confidentiality, integrity, and availability of DOL data.

We recommend the CIO:

2. Develop and implement a validation of the provisioned exemptions to ensure all provisioned exemptions are provisioned appropriately.

Finding 3: Lack of Multi-Factor Authentication

We found 2 of 15 DOL information systems selected for testing were not configured to enforce MFA. This deficiency occurred because the two legacy information systems required modernization to support MFA enforcement. OCIO was modernizing both applications to enable MFA and tracking the remediation of deficiencies through POA&Ms.

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, "MFA should be integrated at the application layer, such as through an enterprise identity service as described above, rather than through network authentication (e.g., a virtual private network)." The DOL Cybersecurity Policy Portfolio (CPP), Volume 7, Section 2.2.1, also states, "MFA for access to system-specific non-privileged accounts must be through a two-factor PIV credential or other IAL3/AAL3 credential."[19]

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

We recommend the CIO:

3. Complete in progress efforts to modernize impacted systems and subsequently enable multi-factor authentication.

Finding 4: Quarterly CIO FISMA Metrics Submitted Inaccurately

We inspected the DOL CIO FISMA Metrics for Quarter 1 and determined the following three metric questions were stated inaccurately:

- Question 2.3: How many systems enforce (not optional) an MFA credential that is phishing resistant (e.g., FIDO2, PIV) as a required authentication mechanism for enterprise identities?

[19] DOL CPP, Volume 7: Identification and Authentication (IA), Section 2.2.1, Control IA-2(1): Multi-Factor Authentication to non-Privileged Accounts

- Question 2.4: How many systems accept MFA credentials susceptible to phishing (e.g., push notifications, OTP, or use of SMS or voice) as an acceptable authentication mechanism?

- Question 2.5: How many systems (from 1.1.1 and 1.1.2) allow single factor authentication such as user ID and password (e.g., MFA is optional or not available)?

OCIO's consolidation and validation process for the metrics was not operating effectively, resulting in an overstatement of the number of systems that enforce MFA.

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, "MFA should be integrated at the application layer, such as through an enterprise identity service as described above, rather than through network authentication (e.g., a virtual private network)." This memorandum also states, "Federal applications cannot rely on network perimeter protections to guard against unauthorized access. Users should log into applications, rather than networks, and enterprise applications should eventually be able to be used over the public internet."

This finding arose because OCIO misinterpreted OMB's CIO FISMA Metric guidance and Executive Order 14028 regarding the classification of systems with MFA. OCIO classified internal facing systems and required mandatory PIV enforcement to authenticate to the network; however, systems also still utilized username and password when authenticating to the application.

According to the CIO FISMA Metric guidance, "An Agency should not designate a system MFA-enabled unless it has been established that all applications included within the system boundary have been MFA-enabled." Instead of using Metric Question 2.3, OCIO should have used Metric Question 2.5.1[20] to report internal facing systems that allowed username and password authentication and required mandatory PIV enforcement to authenticate to the network.

Due to this error, DOL misreported its adoption of MFA to OMB.

[20] CIO FISMA Metric Question 2.5.1: How many of the 2.5 systems that allow user ID/password are internal facing and have mandatory PIV access enforced to get on the network where the system resides?

We recommend the CIO:

4. 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.

Finding 5: Application Audit Log Review Not Performed

For 1 of 15 information systems selected for testing, OCIO did not perform monthly reviews of application-level audit logs to identify and investigate potentially inappropriate privileged user activity.

The system security plan for the impacted information system states that the information system administrators must review the audit logs at least monthly to identify abnormal or unusual activity.

We were informed by OCIO that this finding occurred due to a lapse in the professional service that was contracted to implement the system's log viewer tools. Even though the professional service had lapsed, the information system continued to operate.

The absence of privileged application-level audit log reviews increases the risk that unauthorized access and/or activities go undetected. This could result in the misuse or mishandling of the affected system and its data.

We recommend the CIO:

5. Assign appropriate resources to perform the audit log reviews as required by the system security plan.

Protect – Data Protection and Privacy

Finding 6: Lack of Data-At-Rest Encryption

Of 44 DOL servers selected for testing, 5 servers were not configured to encrypt data-at-rest. These servers were not in compliance with Executive Order 14028 requirements, which states that 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.

This finding occurred because OCIO did not modernize legacy servers to allow for the enablement of encryption of data-at-rest.

The absence of data-at-rest encryption may lead to an increased risk of unauthorized access to production data in the event of a cybersecurity breach. This could result in unauthorized updates to, misuse of, or mishandling of DOL data.

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

- Implement data encryption configurations/solutions at the server level for data-at-rest for sensitive information (PII). (FY 2019, Recommendation 15)

Finding 7: Lack of Privacy-Focused, Role-Based Training

OCIO's Cybersecurity Directorate did not require employees and contractors with significant privacy responsibilities to complete specific privacy-focused, role-based training before: (1) accessing information systems and data and (2) performing assigned duties. Additionally, annual role-based privacy refresher training was not required for these employees or contractors.

DOL's Privacy Office, which was established in FY 2024 in the Division of IT Governance, did not inherit specific privacy-focused, role-based training to provide to DOL personnel, as required by the CPP. The Privacy Office will be standing up trainings in the future.

DOL CPP, Volume 2*:* Awareness and Training (AT), Section 2.3.5,[21] states:

> The Division of Information Security Policy and Planning (DISPP) shall provide all users, including managers, senior executives, and contractors, with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

Prior to the establishment of the Privacy Office, the Cybersecurity Directorate of OCIO was responsible for providing privacy-focused, role-based training. According to OCIO, this Cybersecurity Directorate determined the entity-wide Cybersecurity and Privacy Awareness Training as sufficient to meet the

[21] DOL CPP, Volume 2: Awareness and Training (AT), Section 2.3.5, Control AT-3(5): Role Based Training: Processing Personally Identifiable Information

requirement for role-based training for employees with responsibilities handling PII. Therefore, specific privacy-focused, role-based training was not completed by individuals with significant PII responsibilities.

The lack of specific privacy-focused, role-based training for employees and contractors with significant privacy responsibilities—prior to granting system access and performing assigned duties—may lead to potential privacy breaches. This could result in the unauthorized access, misuse, or mishandling of DOL sensitive data, potentially violating privacy laws and regulations.

We recommend the CIO:

6. Develop, implement, and track privacy-focused, role-based training for employees and contractors with significant privacy responsibilities.

Protect – Security Training

Finding 8: Training Management System was Configured Incorrectly

OCIO was unaware that an individual did not receive required training until identified as part of this performance audit. Specifically, of 25 selected users selected for testing, 1 user did not complete the 2023 Annual Cybersecurity and Privacy Training before the start of FY 2024. OASAM performed ineffective oversight over the LearningLink[22] Service Provider and did not ensure that newly onboarded users were correctly added to the LearningLink system and training was administered. If an employee is not configured in LearningLink appropriately, then they will not receive all the required trainings.

According to DOL CPP, Volume 2: Awareness and Training, Section 2.2,[23] security awareness training is required as part of initial training for new users and annually thereafter.

The finding occurred because OCIO did not implement a control to verify that individuals were correctly entered into LearningLink, which is needed to automatically enroll individuals in the correct training plans.

[22] LearningLink is an external system that is used to establish learning plans for employees, which includes required training.
[23] DOL CPP, Volume 2: Awareness and Training, Section 2.2, AT-2: Literacy Training and Awareness

Without proper training, users may lack awareness of common cyber threats, such as phishing emails, social engineering attacks, or malware. Cybersecurity awareness training equips users with knowledge and skills to identify and respond to potential threats. A lack of such training increases risks to the availability, integrity, and confidentiality of DOL data.

We recommend the CIO:

7. Develop and implement validation controls to ensure users are properly onboarded to LearningLink and assigned required trainings.

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 five Cybersecurity Framework Function areas outlined in the FY 2024 IG FISMA Metrics. We responded to the FY 2024 IG FISMA 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 Group 2; 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[24] selection of 20 information systems (15 federal and 5 contractor information systems) from a total population of 73 information systems from DOL's FISMA inventory as of January 1, 2024. We selected 15 IT Shared Services federal systems and 5 non-IT Shared Services federal systems. We also selected three IT Shared Services federal systems and two non-IT Shared Services federal systems as a part of our additional testing of one ISCM metric question. 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 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.

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

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

Tests of internal controls must be sufficiently extensive to provide reasonable assurance that the controls being tested were suitably designed and operated effectively throughout the period under audit. 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 the Government Accountability Office'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: Government Accountability Office'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 five Cybersecurity Framework Functions and nine FISMA Metric Domains from the Core Metrics and Supplemental Metrics Group 2:

- 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 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 nine FISMA Metric Domains. If we identified findings associated with metrics that were tested in consideration of Maturity Level 3 questions, we considered the nature of the identified finding(s) and assessed the maturity at Level 1 (Ad-hoc) or Level 2 (Defined) for the questions with responses indicating control failures.

- For metrics determined to be at Maturity Level 3, we performed further procedures leveraging Maturity Level 4 (Managed and Measurable) questions within the nine FISMA Metric Domains. If we identified findings associated with metrics that were tested in consideration of Maturity Level 4 questions, we 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 nine FISMA Metric Domains. We performed these procedures to evaluate the design of the metrics. If we identified findings associated with metrics that were tested in consideration of Maturity Level 5 questions, we assessed the maturity at Level 4 for the questions with responses indicating control failures.

Based on the results of our test procedures, we input the maturity level for each of the Core Metrics and Supplemental Metrics Group 2 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 Group 1 and Group 2 were averaged independently to determine a domain's maturity calculation. The calculated average scoring model was used for FY 2024. 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 from December 14, 2023, through June 30, 2024. All testing was performed through virtual meetings, walk-throughs, and observations with DOL representatives. Additionally, we held regular status meetings with DOL management 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 SP 800-53, Rev. 5.1, Rel 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 SOP to evaluate DOL's controls supporting CSP monitoring.

APPENDIX B: KPMG'S ANALYSIS OF THE AGENCY'S RESPONSE

We appreciate DOL OCIO's (management) response to the findings and conclusions reported in connection with the FY 2024 DOL FISMA performance audit. In its response, management generally concurred with our findings and recommendations; however, management disagreed with our conclusion that DOL's information security program was ineffective.

We considered management's response, reflected on our findings, and affirmed that we correctly applied the FY 2023–2024 Inspector General FISMA Reporting Metrics (Guidance) in assessing evidence and making determinations that:

- Five of the nine FISMA metric domains (SCRM, CM, IAM, DPP, and CP) were assessed as Consistently Implemented (Level 3).
    - Management cited its work to close four recommendations related to Vulnerability and Patch Management, but three additional recommendations relating to secure configuration settings were not remediated and resulted in the CM domain being rated as ineffective.
- DOL's information security program was ineffective based on the Guidance's definition of an effective program, which states that achieving a Managed and Measurable (Level 4) maturity rating or above represents an effective level of security.

Additionally, we noted that in its response, management described accomplishments outside the scope of our performance audit. Specifically:

- Management mentioned its implementation of OMB Memorandum M-24-10, which includes security control requirements associated with federal agencies' use of artificial intelligence. These requirements were not addressed in the Guidance and were not included in our audit scope. Therefore, we did not validate management's claims about its implementation of OMB Memorandum M-24-10 requirements.
- Management cited its achievement of an overall Federal Information Technology Acquisition Reform Act (FITARA) score of "A" as an accomplishment of its information security program. Management self-attested its FITARA score, and FITARA scoring requirements were not included in the Guidance. Thus, we did not validate management's claims related to its FITARA score.

As a result, after reviewing management's response, we did not modify our findings, recommendations, maturity level assessments for the FY 2024 IG FISMA Reporting Metrics, or overall conclusion that DOL's information security program was ineffective based on the criteria in the Guidance.

APPENDIX C: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

MEMORANDUM FOR: CAROLYN RAMONA HANTZ
Assistant Inspector General for Audit

FROM: LOUIS CHARLIER
Acting Chief Information Officer

LOUIS CHARLIER
Digitally signed by LOUIS CHARLIER
Date: 2024.10.21 18:10:45 -04'00'

SUBJECT: Management Response to DRAFT REPORT – (Fiscal Year) FY 2024 FISMA DOL Information Security Report: 23-25-002-07-725

This memorandum responds to the above-referenced *Draft Report – FY 2024 FISMA DOL Information Security Report: 23-25-002-07-725*, issued October 4, 2024. Information security continues to be a top priority at the Department, and DOL leadership remains committed to continuously strengthening DOL's information security posture. DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve upon within the information security program and is actively working to address those areas.

Management generally concurs with the findings identified during the FY 2024 FISMA audit evaluation and described in the draft report. In all cases, we have either since addressed the associated recommendations or have developed plans to address them in FY 2025. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).

Although the result of the audit, following the Office of Management and Budget's guidance, determined that the Department of Labor's (DOL) information security program falls short of being effective, we firmly assert the contrary, backed by substantial evidence of our program's efficacy and continuous improvement. Our advancements in Information Security Continuous Monitoring (ISCM) and Vulnerability Management are testament to our unwavering efforts in fortifying our information security framework. The creation of tiered reports and the significant improvements in our vulnerability remediation process serve as strong proof of our forward momentum, offering both the quantitative and qualitative metrics of our effectiveness. It's noteworthy that 68% of the Inspector General's metrics were rated as Effective, underscoring our program's robustness. Furthermore, DOL's ability to resolve numerous recommendations from previous years showcases our proactive and diligent efforts in rectifying identified weaknesses.

Our adoption of a risk-based strategy, in line with NIST recommendations and M-24-04 guidelines, highlights DOL's commitment to implementing a dynamic and resilient information security practice capable of adapting to the ever-changing threat landscape. This strategic approach not only addresses minor compliance discrepancies but also significantly contributes to the overarching success and effectiveness of our information security program.

In Fiscal Year 2024, DOL made significant strides in enhancing its information security program, particularly in areas emphasized by Executive Order 14028, "Improving the Nation's Cybersecurity." Our ongoing initiatives to deploy enterprise-wide encryption for data-at-rest and in-transit, alongside the implementation of multifactor authentication, are pivotal to our cybersecurity framework. Our collaboration with the Department of Homeland Security in rolling out the Continuous Diagnostics and Mitigation (CDM) capability, coupled with our effective use of the Technology Modernization Fund to advance a zero-trust architecture, are critical milestones in meeting the Executive Order's mandates. Given these comprehensive enhancements and strategic initiatives, we stand by our

position that the DOL's information security program is not only effective but also exemplifies a model of continuous improvement and adaptability in the face of evolving cybersecurity challenges.

DOL accomplished the following additional information security results during FY 2024:

- During the FY 2024 FISMA Audit, DOL worked with OIG to close 18 prior year (PY) IT audit recommendations, reducing the number of open PY recommendations by more than 55 percent. Specifically, 4 of the recommendations closed were related to Vulnerability & Patch Management, which is a testament to DOL's enhanced vulnerability remediation procedures and in support of the DHS DOL CDM initiative.
- Held DOL-wide Cybersecurity Awareness Month program as well as other ongoing awareness campaigns, role-based training, and All-Staff notifications to reinforce cybersecurity knowledge.
- Addressed emerging federal information security risks, particularly those targeted by OMB Memoranda released in recent years, such as OMB M-24-10 (*Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*).
- Developed a risk-based approach to identify high-value assets (HVA) through collaborative, data-driven prioritization, which led to resource allocation based on system categorization and ensured the protection of these assets.
- Collaborated with CISA on penetration testing efforts and adopted continuous monitoring to identify previously unknown vulnerabilities. Additionally, DOL continues to participate in the CISA Vulnerability Disclosure Policy (VDP) Platform.
- Achieved an overall "A" on the Federal Information Technology Acquisition Reform Act (FITARA) 18.0 Scorecard, an improvement from a previous "B." The FITARA scorecard, released twice a year, provides a snapshot of the IT strategies of the 24 largest government agencies. DOL exceeded the average score in nearly all categories, including Cybersecurity.

Looking ahead, DOL will continue to focus on strengthening its information security, prioritizing the following:

- Complete adoption of multifactor authentication and encryption of data-at-rest and in-transit.
- Enhance DOL's enterprise log management capability in accordance with OMB M-21-31.
- Implement Security Operations Center enhancements that will allow the Department to anticipate and mitigate risk and stay ahead of the evolving threat landscape.
- Advance the monitoring and protection of critical software and the maturing of capabilities for supply chain risk management.
- Finalize the implementation of data loss prevention tools and alerts.
- Continue efforts to transition DOL's most critical and sensitive networks and systems to quantum resistant cryptography.
- Proceed to increase DOL's capacity to responsibly adopt Artificial Intelligence (AI).
- Continue to transition DOL's network infrastructure to Internet Protocol Version 6.
- Continue the deployment of automation tools and emerging technologies to detect and mitigate cyber threats, to include integrating a zero-trust architecture to better protect resources from unauthorized access.

As demonstrated in the enclosed FISMA report, DOL has implemented a robust information security program and plans to further improve its information security posture consistent with OIG recommendations. The Department recognizes that our work in this space is ongoing due to the ever-evolving nature of the threats.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202) 693-4446 or have your staff contact Paul Blahusch, Chief Information Security Officer

(CISO), at blahusch.paul.e@dol.gov or (202) 693-1567. As the CISO, Paul Blahusch is responsible for the corrective actions identified in this correspondence.

cc: Carolyn Angus-Hornbuckle, Assistant Secretary for Administration and Management
Vince Micone, Deputy Assistant Secretary for Operations
Paul Blahusch, Chief Information Security Officer
Muhammad Butt, Division Chief for Cybersecurity Governance

APPENDIX D: FINDING REFERENCE

Finding No.	Function	Domain	Issued Finding
1	Identify	Supply Chain Risk Management	FISMA-24-03
2	Protect	Identify and Access Management	FISMA-24-01
3	Protect	Identity and Access Management	FISMA-24-05
4	Protect	Identity and Access Management	FISMA-24-08
5	Protect	Identity and Access Management	FISMA-24-07
6	Protect	Data Protection and Privacy	FISMA-24-06
7	Protect	Data Protection and Privacy	FISMA-24-02
8	Protect	Security Training	FISMA-24-04

APPENDIX E: STATUS OF PRIOR YEAR RECOMMENDATIONS

As part of the FY 2024 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 a recommendation had been sufficiently implemented and there were no related issues identified during our FY 2024 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 2024, we determined there were 19 open prior year FISMA recommendations. Based on our testing, we determined 10 recommendations were closed, and 9 recommendations remained open.

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

Related Domain	Report Year	Prior Year Recommendation	Status of Recommendation
RM	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**
RM	2019	Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner.	**Closed**
RM	2022	Update DOL entity-wide and system-level security policies, procedures, and plans to comply with NIST SP 800-53, Rev. 5.	**Open**
RM	2023	Develop and implement compliance controls to identify whether systems have performed the quarterly POA&M review.	**Closed**

Related Domain	Report Year	Prior Year Recommendation	Status of Recommendation
SCRM	2023	Review applicable NIST documentation and update the related SCRM policies and strategy accordingly. Further, ensure leadership with SCRM roles and responsibilities perform a thorough review of the policy	**Closed**
CM	2019	Develop and implement performance metrics for configuration management.	**Open**
CM	2019	Design and implement controls to monitor DOL assets for missing patches, service packs, hot fixes, and other software updates that are not associated with a CVE.	**Closed**
CM	2020	Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process.	**Closed**
CM	2020	Implement a process for approving deviations from established configuration settings.	**Open**
CM	2021	Enforce DOL requirements for implementing, auditing, testing, and documenting exceptions to baseline configurations.	**Open**
CM	2021	Execute the OCIO and AO oversight process to ensure compliance with DOL requirements for the performance of SIAs prior to the implementation of system changes.	**Closed**
CM	2021	Implement a centralized process to monitor vulnerabilities for information systems to ensure that each vulnerability is remediated within the CSH defined timeframe.	**Closed**

Related Domain	Report Year	Prior Year Recommendation	Status of Recommendation
CM	2022	Implement proper quality control to ensure change management processes are being performed for all systems and equipment on the DOL network.	**Closed**
DPP	2019	Implement data encryption configurations and solutions at the server level for data-at-rest for sensitive information (PII).	**Open**
IAM	2019	Finalize the implementation of the access control technologies.	**Open**
IAM	2023	Develop and implement compliance review controls to ensure users re-acknowledge the RoB after updates are made and to identify users that have not re-acknowledged the RoB.	**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**
DPP	2022	Implement data loss prevention tools and alerts based on the results of agencies' data exfiltration tests.	**Open**
CP	2021	Enhance the OCIO monitoring and oversight of system owners to complete BIAs.	**Closed**

APPENDIX F: ACRONYMS AND ABBREVIATIONS

Acronym / Abbreviation	Definition
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
BIA	Business Impact Analysis
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
CPP	Cybersecurity Policy Portfolio
CSH	Computer Security Handbook
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
DHS	U.S. Department of Homeland Security
DOL	U.S. Department of Labor
DPP	Data Protection and Privacy
ESD	Enterprise Service Desk
FAM	Financial Audit Manual
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquistion Reform Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IAM	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

Acronym / Abbreviation	Definition
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identification Verification
POA&M	Plan of Action and Milestones
Rel.	Release
Rev.	Revision
RM	Risk Management
RoB	Rules of Behavior
SCRM	Supply Chain Risk Management
SIA	System Impact Analysis
SOP	Standard Operating Procedure
SP	Special Publication
ST	Security Training

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