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

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2023 FISMA DOL INFORMATION SECURITY REPORT: MAKING IMPROVEMENTS TOWARD AN EFFECTIVE 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 06, 2023
REPORT NUMBER: 23-24-001-07-725

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

BRIEFLY...

FY 2023 FISMA DOL INFORMATION SECURITY REPORT: MAKING IMPROVEMENTS TOWARD AN EFFECTIVE PROGRAM

December 06, 2023

WHY OIG CONDUCTED 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.

WHAT OIG DID

We contracted with KPMG LLP (KPMG) to conduct an independent performance audit on DOL's Fiscal Year (FY) 2023 information security program for the period October 1, 2022, through June 30, 2023. To determine the effectiveness of the program, we evaluated security controls in accordance with applicable legislation, guidelines, directives, and other documentation. Findings were also based on testing relevant security controls and targeted penetration tests.

WHAT OIG FOUND

KPMG reported seven findings for DOL's information security program within two of five Cybersecurity Framework Functions and four of nine FISMA Metric Domains, which resulted in determining DOL's information security program was not effective, according to guidance from the Office of Management and Budget.

Although DOL established and maintained its information security program, 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 Cybersecurity Framework Functions: Identify, Protect, and Recover. A security program is only considered effective if the calculated score of the Cybersecurity Framework Functions is rated at least Managed and Measurable (Level 4).

While the Office of Chief Information Officer (OCIO) has made improvements in its information security program from previous years, we identified areas of improvement required to reach a Managed and Measurable, or effective, program. DOL's information security program did not fully adhere to applicable FISMA requirements and other guidance, and KPMG noted further deficiencies in the development and implementation of supply chain risk management security controls, Plan of Action and Milestones reviews, configuration management controls, and the enforcement of rules of behavior acknowledgement. Based on these issues, we continue to be concerned about the remaining corrections needed in OCIO's oversight and accountability over DOL's information security control environment.

WHAT OIG RECOMMENDED

KPMG made three new recommendations to strengthen DOL's information security program. Based on our testing, we determined that 38 prior year recommendations were closed, and 31 recommendations remained open.

READ THE FULL REPORT

https://www.oig.dol.gov/public/reports/oa/2024/23-24-001-07-725.pdf

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

Gundeep Ahluwalia
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave. 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) 2023 information security program. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal Inspectors General (IG), 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 we 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, 2022, through June 30, 2023. 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. In addition, KPMG performed an external penetration test on two public facing Uniform Resource Locators from 2 of

12 selected IT Shared Services systems. Additional details regarding the scope of the independent audit are included in KPMG's report.

RESULTS

KPMG identified and reported seven 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, which resulted in determining DOL's information security program was not effective according to the Office of Management and Budget guidance.

A security program is considered effective if the calculated score of the FY 2023 Core and Supplemental IG Metrics reported in CyberScope 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.

KPMG also 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, *Security and Privacy Controls for Information System and Organization* (NIST SP 800-53, Rev. 5). KPMG noted further deficiencies in the development and implementation of supply chain risk management security controls, Plan of Action and Milestones reviews, configuration management controls, and the enforcement of rules of behavior acknowledgement.

KPMG made recommendations related to three control deficiencies. KPMG did not make recommendations for the other four control deficiencies because three corresponded to open prior year recommendations and one was previously identified by management and tracked through a Plan of Action and Milestones. KPMG also evaluated the implementation of recommendations from prior IT reports from 2011, 2015, and 2018 through 2022. The IT reports included FISMA performance audits, discretionary audits, and financial statement audits. Out of 69 previously open IT recommendations, KPMG determined DOL successfully closed 38 recommendations and 31 recommendations remained open.

We remain concerned that the prior year finding of compliance with NIST SP 800-53, Rev. 5, remains outstanding. By not updating the Department's policies and procedures to be compliant, the Chief Information Officer is not taking necessary steps in mitigating IT risk for the Department. We are also

concerned about the findings of unimplemented supply chain risk policies and undocumented configuration deviations, which diminish the Chief Information Officer's ability to ensure the foundational steps to manage IT risk for the Department are taken.

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

Carolyn R. Hantz
Assistant Inspector General for Audit

CONTRACTOR PERFORMANCE AUDIT REPORT

Independent Auditor's Performance Audit Report on the Effectiveness of the U.S. Department of Labor's Information Security Program and Practices for Fiscal Year 2023

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

This report presents the results of our independent performance audit of the U.S. Department of Labor's (DOL) information security program and practices for its information systems. We conducted our performance audit from November 1, 2022, through October 21, 2023, and our scope focused on the period of October 1, 2022, through June 30, 2023.

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 the effectiveness of 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) 2023 Inspector General (IG) FISMA Metrics.[1] We responded to the FY 2023 Core IG FISMA Metrics and

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

FY 2023 Supplemental IG FISMA Metrics and assessed the maturity levels on behalf of the DOL Office of Inspector General (OIG). We also followed up on the status of prior year recommendations.

Based on the maturity levels calculated in CyberScope[2] and Office of Management and Budget (OMB) guidance, we determined DOL's information security program was not effective. A security program is considered effective if the calculated average of the FY 2023 IG FISMA Core Metrics and FY 2023 IG FISMA Supplemental Metrics is at least Managed and Measurable (Level 4). Table 1 depicts DOL's assessed maturity levels for the five Cybersecurity Framework Functions in FY 2023.

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 2023 Inspector General Section Report for DOL

During FY 2023, we tested security controls at the entity level and for a selection of 20 systems. We also performed an external penetration test on two public facing Uniform Resource Locators (URL) from 2 of 12 selected information technology (IT) Shared Services systems. The external penetration test was performed as of June 21, 2023. For five additional information systems, we performed testing over one Information System Continuous Monitoring metric question related to ongoing information system assessments.

[2] CyberScope, operated by the Department of Homeland Security (DHS) on behalf of OMB, is a web-based application designed to streamline information technology security reporting for federal agencies. It gathers and standardizes data from federal agencies to support FISMA compliance. In addition, IGs provide an independent assessment of effectiveness of an agency's information security program. OIGs must also report their results to DHS and OMB annually through CyberScope.

We also performed procedures to test the completeness and accuracy of information used by management for a selection of metrics from the FISMA Chief Information Officer (CIO) Metrics[3] Reporting to OMB for Quarter 2 of FY 2023.

We identified seven 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 when we assessed the maturity levels for each of the FY 2023 Core and Supplemental IG FISMA Metrics, 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 "not effective."

DOL's system-level security policies still have not been updated to comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information System and Organization* (NIST SP 800-53, Rev. 5). We noted further deficiencies in the development and implementation of supply chain risk management security controls, Plan of Action and Milestones (POA&M) reviews, configuration management controls, and the enforcement of rules of behavior (ROB) acknowledgement.

In response to these control deficiencies, we made three recommendations related to strengthening DOL's information security program. We did not make recommendations for three other control deficiencies as they corresponded to open prior year recommendations. We did not make a recommendation for the seventh control deficiency included in this report because it was previously identified by management and tracked through a POA&M.

We suggest that DOL implement a process to determine if these recommendations apply to other information systems maintained in its FISMA inventory. Furthermore, we recommend that the Office of the Chief Information Officer (OCIO) implement robust monitoring capabilities to continually assess the security state of its systems to include a process for identified compliance gaps.

We also evaluated the implementation of recommendations from prior IT reports from 2011, 2015, and 2018 through 2022. The IT reports included those

[3] The FISMA CIO Metrics provide the data needed to monitor agencies' progress towards the implementation of the Administration's priorities and best practices that strengthen Federal cybersecurity. Achieving the metrics alone will not address every cyber threat, and agencies will need to implement additional defenses to effectively manage their cybersecurity risks. For more information see: FY 2023 CIO FISMA Metrics, Version 2.0 (June 2023), available at: https://www.cisa.gov/sites/default/files/2023-06/FY23_FISMA_CIO_Metrics_v2_May-2023-Final_508.pdf.

prepared in connection with previous FISMA performance audits, discretionary audits, and financial statement audits. Out of 69 previously open recommendations, we determined DOL successfully closed 38 recommendations.

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

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

KPMG LLP

November 29, 2023

BACKGROUND

We performed the FY 2023 FISMA evaluation 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 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 its mission. OCIO has four strategic goals in support of DOL's mission:

1. **Create DOL IT platform services:** Create an integrated platform that links hardware, applications, and data and provides strategic capabilities to achieve DOL-wide operational efficiencies to serve the wage earners, job seekers, and retirees of the United States more effectively.

2. **Modernize legacy applications:** Drive the modernization of legacy agency mission-critical applications by delivering technology leadership and modern solutions, resulting in a state-of-the-art end-user experience, optimized functionality, and increased security.

[4] DOL Contract Number: 1604DC-20-A-0014

3. **Secure and enhance the IT infrastructure:** Integrate and standardize DOL's IT infrastructure to provide a robust cybersecurity posture while increasing the reliability and functionality of DOL's information systems and infrastructure that support mission-critical services.

4. **Transform the customer experience:** As DOL's IT service provider, deliver leading IT services and solutions to enable DOL agencies to provide superior support to the American Public.

Within DOL OCIO, the Directorate of Cybersecurity is tasked with securing DOL's information systems and implementing effective cybersecurity governance, compliance, and protection of DOL IT infrastructure and data so agency missions are not compromised.

The Directorate of Cybersecurity implements solutions to achieve the following:

- **Stop data theft:** Preventing unauthorized copying, transferring or retrieval of data from a computer or server

- **Control Access:** Deploying an advanced tool called the Identity Service Engine to control network access

- **Filter Content:** Limiting views to certain URLs or websites to deliver an essential layer of protection from malware, phishing, and other online scams

- **Prevent Intrusions:** Using threat prevention technology to examine network traffic flows as well as detect and prevent vulnerability exploits

FISMA IG METRICS AND REPORTING

The Council of the Inspectors General on Integrity and Efficiency, in coordination with OMB, DHS, the Federal Chief Information Officers council, and the Chief Information Security Officers council, developed the FY 2023 Core IG FISMA Metrics and FY 2023 Supplemental IG FISMA Metrics[5] based on the five Cybersecurity Framework Functions outlined in the NIST's *Framework for*

[5] OMB, "FY 2023–2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics"

Improving Critical Infrastructure Cybersecurity[6] (herein referred to as the Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.[7]

The FY 2023 Core and Supplemental IG FISMA Metrics were chosen based on alignment with Executive Order (EO) 14028 (specifically the Multifactor Authentication section and the Encryption and Software Supply Chain Security and Critical Software section),[8] as well as OMB guidance provided to agencies to further modernize federal cybersecurity. OMB also provided the following guidance:

- 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]
- 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. These Functions are: Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management.
[7] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," issued on February 12, 2013, established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the EO calls for the development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and leading practices to help organizations manage cybersecurity risks. The resulting framework, created through collaboration between the government and the private sector, uses a common language to address and cost-effectively manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses.
[8] Executive Order 14028, "Improving the Nation's Cybersecurity," issued May 12, 2021
[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 2-year cycle—as agreed to by the Council of the Inspectors General on Integrity and Efficiency, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency. The rotating 2-year cycle metrics are denoted as the "FY 2023 Supplemental Metrics" and "FY 2024 Supplemental Metrics." 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 security programs, and contribute to the overall evaluation and determination of security program effectiveness.

The FY 2023 Core IG FISMA Metrics and Supplemental IG FISMA Metrics use a capability maturity model developed by OMB, DHS, the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders for the nine FISMA Metric Domains. Table 2 outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domains.

[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

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

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 and other data points 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 rating for each FISMA Metric Domain and Cybersecurity Framework Function. The maturity 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 IG FISMA Metrics Reporting guidance, a security program is considered effective if the calculated average of the FY 2023 Core and Supplemental IG

[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.

Metrics reported in CyberScope is at least Managed and Measurable (Level 4).

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 maturity levels calculated in CyberScope, we determined DOL's information security program was not effective as it did not fully adhere to applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines. A security program is considered effective if the calculated average of the FY 2023 Core and Supplemental IG FISMA Metrics 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 2023 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 2023 DOL CyberScope Response

During FY 2023, we tested security controls at the entity level and for a selection of 20 systems. We also performed an external penetration test on 2 public facing URLs from 2 of 12 selected IT Shared Services systems. The penetration test was performed as of June 21, 2023. We did not identify high or critical vulnerabilities; however, we noted internal disconnect between DOL teams—specifically, between the DOL Enterprise Security Operation Center, which is responsible for detecting and monitoring vulnerabilities, and OCIO agency technical teams, which are responsible for developing and implementing vulnerability resolutions.

For five additional information systems, we performed testing over one ISCM metric question related to ongoing information system assessments.

We inquired with OCIO management and requested corresponding evidence to test the completeness and accuracy of information used by management for a selection of CIO metrics from the CIO FISMA Reporting to OMB for Quarter 2 of FY 2023. Specifically, we selected CIO metrics related to prior year recommendations, EO 14028, and OMB Memorandum M-22-09. We determined that OCIO utilizes the CIO FISMA Reporting Standard Operating Procedure (SOP) to document the procedures the Division of Information Security Policy and Planning implemented to collect and report the information used in the FISMA CIO Reporting to OMB for Quarter 2 of FY 2023. OCIO Security sent out a data call to DOL agencies, reviewed the information collected, and tracked issues as identified in an issue log until remediated.

However, OCIO did not formally document the details of the review performed, including a confirmation that the review was performed and how the data was

determined to be complete and accurate. OCIO did not compare the data, such as hardware assets, from its authoritative sources to the data provided by the DOL agencies. Further, OCIO did not consistently track reporting issues through their established issue resolution process. We identified issues that were resolved through informal channels and were not documented in the issue resolution log.

While OCIO made improvements to its information security program, we identified areas of improvement required to reach a Managed and Measurable, or effective, program. For example, OCIO's system-level security policies have not been updated to comply with NIST SP 800-53, Rev. 5. Additionally, we noted that OCIO did not implement the SCRM security controls defined in its policies and procedures, as the documented SCRM security controls did not have robust statements to ensure accurate implementation or had not been implemented at all. We noted further deficiencies in the development and implementation of SCRM security controls, POA&M reviews, configuration management controls, and the enforcement of ROB acknowledgement.

We also evaluated the implementation of recommendations from prior IT reports from 2011, 2015, and 2018 through 2022. The IT reports included FISMA performance audits, discretionary audits, and financial statement audits. Out of 69 previously open recommendations, we determined DOL successfully closed 38 recommendations.

As a response to deficiencies identified in past FISMA performance audits, OCIO implemented monthly continuous monitoring reports in December 2022 to enhance its oversight at the three organizational tiers: system, agency, and organization. These reports included performance metrics to measure the effectiveness across the domain areas; however, OCIO did not identify metrics and measures for both IT Shared Services systems and non-IT Shared Services systems that are oriented to driving security outcomes versus binary metrics. As DOL's information security program evolves and performance data becomes more readily available, it is vital that OCIO develop and capture program effectiveness, efficiency, and impact measures to align with NIST SP 800-55, Rev 1.[14] Further, it is important that OCIO ensure targets for all measures and metrics are defined in accordance with DOL's risk tolerance for its control environment.

[14] NIST, "Performance Measurement Guide for Information Security," SP 800-55, Rev 1. (July 2008)

IDENTIFY

The objective of the Identify Function in the Cybersecurity Framework 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; however, OCIO did release the Cybersecurity Policy Portfolios (CPP)[15] for DOL in January 2023 to be compliant with NIST SP 800-53, Rev. 5. Further, OCIO implemented policies and processes to assess and review supply chain risks. However, OCIO did not fully implement all SCRM security controls, and SCRM security controls reflected in policies did not include robust implementation statements to ensure accurate implementation.

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 Consistently Implemented (Level 3). 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.

[15] The Cybersecurity Policy Portfolios specify the Departmental cybersecurity policy, standards, procedures, and guidance relating to each of the NIST control families and other relevant federal requirements.

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. However, for one IT Shared Services system, management did not perform the quarterly POA&M review, in accordance with the DOL CPP.

In addition, OCIO utilized an automated tool to capture information from incident response tools to perform scenario analyses and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to DOL systems and data.

OCIO deployed and began using the DHS Continuous Diagnostic and Mitigation Logical Data Model. As of February 2023, OCIO met the requirements set by DHS for 80 percent of government furnished equipment to be reported through the Continuous Diagnostic and Mitigation dashboard by April 2023. While the dashboard was not fully implemented into production until April 2023, DOL utilized the dashboard prior for data collection. DOL's Logical Data Model captures data attributes on hardware, software, and risk within a dashboard to provide near real-time visibility across DOL's network.

As of January 2023, OCIO implemented the CPPs at the Department level to comply with NIST SP 800-53, Rev. 5; however, for 11 of 15 information systems selected for testing, OCIO did not update the DOL system-level policies and procedures, including system security plans that were completed after January 3, 2023. OCIO created a POA&M to document and track the deficiency and maintained a plan with a phased approach to update all system policies and procedures by June 30, 2023; as of June 30, 2023, that POA&M remained open.

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 ensure appropriate contractual requirements are included for acquisitions. We tested the third-party monitoring checklists for five contractor systems and determined that 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 Defined (Level 2). OCIO consistently implemented a process to review and monitor third-party providers. OCIO developed SCRM standards and procedures as a part of the CPP; however, it did not address all elements of NIST SP 800-53, Rev. 5, regarding SCRM security controls. Specifically, the CPP, Volume 20, "Supply Chain Risk Management Standards and Procedures," did not: define the control for protecting the SCRM plan from unauthorized disclosure and modification, define the unambiguous expression of the supply chain risk appetite and tolerance for DOL, or include sufficient detail in the purpose and scope of the SCRM Plan and Strategy.

PROTECT

The objective of the Protect Function in the Cybersecurity Framework is to develop and implement appropriate safeguards to ensure 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 has implemented procedures and policies for CM, IAM, DPP, and ST, our testing found issues in the implementation and effectiveness of controls in the CM and IAM domains.

CONFIGURATION MANAGEMENT

FISMA requires agencies to develop an information security program that includes policies and procedures to ensure 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 Consistently Implemented (Level 3). While we noted OCIO developed and implemented CM policies and procedures, we found issues—related to prior year recommendations—with the baseline configuration deviation process and the vulnerability and patch management process. The system owner did not perform static application scanning on one IT Shared Services system and one non-IT Shared Services system. OCIO required system owners to perform static application scanning on their respective systems, which

uses software to analyze the source code of a system to identify vulnerabilities; however, OCIO did not enforce the requirement for static application scanning on all systems.

OCIO implemented automated tools to assess baselines and configurations settings of its information systems. These tools gave OCIO near real-time insight and monitoring capabilities of its information systems and the ability to generate reports to identify compliant and non-compliant devices. While OCIO developed an Operating System Baseline Creation SOP, which included a deviation process, OCIO did not consistently document or approve identified deviations from defined baselines within the baseline documentation.

OCIO implemented a Trusted Internet Connection 2.0 program to protect the DOL network. However, OCIO is in the process of implementing the Trusted Internet Connection 3.0 solution identified, in accordance OMB Memorandum M-19-26.[16]

OCIO implemented a robust vulnerability disclosure program for all DOL internet-accessible federal systems to allow users to report and resolve bugs or vulnerabilities. OCIO centrally manages the vulnerabilities reporting to DHS via "Binding Operational Directive 22-01, Know Exploited Vulnerability (KEV)," for IT Shared Services systems and non-IT Shared Services systems.

OCIO centrally managed its flaw remediation process and monitored, analyzed, and reported qualitative and quantitative performance measures on the effectiveness of its flaw remediation processes for IT Shared Services systems selected for testing. However, OCIO did not continuously monitor the flaw remediation process for non-IT Shared Services systems selected for testing, including vulnerability scanning configurations and scanning results for non-KEV vulnerabilities. In addition, for two IT Shared Services systems, OCIO did not patch three high and two critical non-KEV vulnerabilities, in accordance with the timeframe defined in the DOL CPP.

IDENTITY AND ACCESS MANAGEMENT

The IAM Domain includes the requirement that an agency must implement a set of capabilities to ensure that users authenticate to 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

[16] OMB, "Update to the Trusted Internet Connections (TIC) Initiative," M-19-26 (September 12, 2019), available at: https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf

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 (ICAM).

Based on the results of our procedures, we assessed DOL's IAM FISMA Metric Domain as Managed and Measurable (Level 4). 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 made progress toward automating privileged account management by enhancing its tools and capabilities. For example, OCIO was in the process of implementing a tool to support the automation of privileged account management in a phased approach across DOL. Nonprivileged account creation and provisioning was enhanced through automated mechanisms and tools. OCIO began the deployment of privileged account management tools; however, the automated solution was not deployed across the Department. OCIO also did not utilize an automated solution for privileged account creation and recertification. Additionally, one IT Shared Services system did not ensure all users re-signed the updated annual ROB, as required by the CPP.

OCIO developed and implemented an ICAM roadmap. The roadmap detailed current and future technologies for DOL to implement to improve its security posture. OCIO also utilized this roadmap and its ICAM strategy to assign IAM stakeholders and enforce consistent communication between the stakeholders and DOL leadership.

OCIO implemented tools and processes to further enhance its authentication capabilities to access DOL's networks and systems for nonprivileged and privileged users, including Single Sign-On and a variety of multifactor authentication mechanisms. In accordance with EO 14028, OCIO developed a Zero Trust Architecture plan and was implementing cloud solutions to move toward zero trust. In addition, OCIO utilized controls to monitor and manage remote access.

We also performed an external penetration test on two public facing URLs from 2 of 12 selected IT Shared Services systems. Testing techniques included, but were not limited to, the performance of vulnerability scanning and testing for default or commonly used passwords. We did not identify significant vulnerabilities or issues during this testing.

DATA PROTECTION AND PRIVACY

DPP refers to a collection of activities focused on the security objective of confidentiality, the preservation of authorized restrictions on information access, and the protection of improper disclosure of personal privacy and proprietary information. Effectively managing the risk to individuals 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 the information systems that process, store, and transmit the information. As such, OMB Circular A-130,[17] 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, EO 13719[18] requires agency heads to designate a senior agency official for privacy who is responsible and accountable for the agency's privacy program.

Based on the results of our procedures, we assessed DOL's DPP FISMA Metric Domain as Managed and Measurable (Level 4). OCIO had a privacy program in place for the protection of PII and other sensitive data. In accordance with EO 13719, OCIO appointed a Senior Agency Official for Privacy, who has overall responsibility for establishing and overseeing the Privacy Program at DOL. OCIO's Privacy Program included quantitative and qualitative performance measures over the effectiveness of its privacy activities, including its maintenance of system PII.

As in the previous year, OCIO did not sufficiently encrypt data-at-rest at the server level, although it did make progress to address this issue. In accordance with EO 14028, and as of February 13, 2023, OCIO reported 82 percent of FISMA-reportable systems implemented encryption of data-at-rest, and 84 percent of systems implemented encryption of data-in-transit.

OCIO developed and implemented a policy for IT Shared Services systems and non-IT Shared Services systems to require annual data exfiltration exercises. However, OCIO is still in the process of implementing data loss prevention tools across IT Shared Services systems and non-IT Shared Services systems to mitigate the gaps identified through previous data exfiltration exercises.

[17] 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
[18] Executive Order 13719, "Establishment of the Federal Privacy Council," issued February 9, 2016

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 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 on the effectiveness of its security awareness and training strategies, plans, and programs by capturing course evaluation statistics, analyzing phishing exercise results, promoting social media campaigns, and updating training based on feedback received from users and evolving threats and risks. However, OCIO did not fully address its identified knowledge, skill, and ability gaps through training or talent acquisition.

DETECT – INFORMATION SECURITY CONTINUOUS MONITORING

The objective of the Detect Function in the Cybersecurity Framework is to implement activities to discover and 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. Further, OCIO held personnel accountable to fulfill their roles and responsibilities through monthly ISCM compliance review reports, as of December 2022.

OCIO's ISCM program facilitated the Ongoing Authorization process and collected security-related information related to, among other things, risk management, contingency planning, vulnerability management, and identity and access management, in ISCM compliance review reports. As noted above, these

reports included performance metrics to measure the effectiveness across the domain areas; however, OCIO should identify metrics and measures for both IT Shared Services systems and non-IT Shared Services systems that promote desired security outcomes rather than report binary metrics.

OCIO implemented the functionality to utilize the system security-related information to ensure its systems under Ongoing Authorization are operating within DOL's risk tolerance, but this was not implemented until May 2023. Therefore, we did not have sufficient evidence to evaluate the implementation effectiveness for this control during the period covered by our performance audit.

RESPOND – INCIDENT RESPONSE

The objective of the Respond Function in the Cybersecurity Framework 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 give 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 incident response 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 (US-CERT) 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 Recover Function in the Cybersecurity Framework is to 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 ensure proper CP. OCIO established CP roles and responsibilities throughout the organization; however, we determined that OCIO did not assess and communicate the effectiveness of its recovery activities to relevant stakeholders.

OCIO used Business Impact Analyses and CP tests and exercises to support CP processes and ensure critical infrastructure and systems were able to support timely recovery and reduce the impact of a cybersecurity incident. However, all 15 DOL information systems selected performed tabletop CP exercises and notification drills, in lieu of functional or automated CP tests.

AUDIT FINDINGS AND RECOMMENDATIONS

IDENTIFY – RISK MANAGEMENT

FINDING 1 – SYSTEM SECURITY POLICIES AND PROCEDURES NOT COMPLIANT WITH NIST SP 800-53, REV. 5

DOL did not update its information system security and privacy policies and procedures to be compliant with NIST SP 800-53, Rev. 5, as required by OMB Circular A-130.

OMB Circular A-130, Appendix I, Section 5, states:

> For non-national security programs and information systems, agencies must apply NIST guidelines unless otherwise stated by OMB. For legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within one year of their respective publication dates unless otherwise directed by OMB. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to meet the

requirements of, and be in compliance with, NIST standards and guidelines immediately upon deployment of the systems.

OCIO informed us that this finding occurred due to the level of effort required to document and implement the controls across all DOL information systems.

NIST SP 800-53, Rev. 5, includes new and updated security control requirements that offer a proactive and systematic approach to ensuring that critical systems, components, and services are sufficiently trustworthy and have the necessary resilience to defend against external attacks, misuse, and/or compromise. When DOL's system security policies and procedures are not updated in accordance with NIST SP 800-53, Rev. 5, DOL's information systems and data are potentially vulnerable to new and emerging threats affecting federal organizations, which result in an increased risk to the confidentiality, integrity, and availability of DOL information systems and data.

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

- Update DOL entity-wide and system-level security policies, procedures, and plans to comply with NIST SP 800-53, Rev. 5. (FY 2022 Recommendation 1)

FINDING 2 – QUARTERLY REVIEW OF POA&MS NOT COMPLETED CONSISTENTLY

For 1 of 12 IT Shared Services systems selected for testing, POA&M review evidence could not be provided for 1 of 2 quarters selected.

The CPP, Volume 18, Section 2.4,[19] states: "POA&Ms [must] be monitored at a minimum on a quarterly basis and updated as events occur." This DOL procedure aligns with the requirements of Security Control PM-4 in NIST SP 800-53, Rev 5.

This finding occurred because OCIO did not have proper compliance controls in place to enforce consistent quarterly POA&M reviews.

Failure to perform quarterly POA&M reviews led to unresolved vulnerabilities with inaccurate milestone updates, which resulted in an increased risk of system

[19] DOL CPP, Volume 18: PM Standards and Procedures, Section 2.4: Program Management (PM)-4: Plan of Action and Milestones Process (January 2023)

comprise and adverse impact to the confidentiality, availability, and integrity of data residing on the information system.

We recommend that the CIO:

1. Develop and implement compliance controls to identify whether systems have performed the quarterly POA&M review.

IDENTIFY – SUPPLY CHAIN RISK MANAGEMENT

FINDING 3 – SUPPLY CHAIN RISK MANAGEMENT POLICIES AND PROCEDURES NOT IMPLEMENTED

DOL's SCRM policies and procedures did not fully address the elements of the in-scope NIST SP 800-50, Rev. 5, SCRM security controls. Specifically, the CPP, Volume 20, "Supply Chain Risk Management Standards and Procedures," did not include:

- procedures for protecting the SCRM plan from unauthorized disclosure and modification;
- defined, unambiguous expression of the supply chain risk appetite and tolerance for DOL; and
- sufficient detail in the purpose and scope of the SCRM Plan and Strategy, such as including DOL's high-level purpose for the strategy and implementation; aligning that purpose with DOL's mission, vision, and values; and providing clear direction around DOL's SCRM priorities and its general approach for achieving those priorities. In addition, DOL did not include details identifying specific roles and responsibilities as they relate to SCRM or the name(s) and contact information for those responsible for the strategy and implementation of the SCRM Plan and Strategy at each level.

Furthermore, OCIO did not implement the SCRM security controls defined in its policies and procedures, as the documented SCRM security controls did not have robust statements to ensure accurate implementation or had not been implemented at all.

NIST SP 800-53, Rev. 5, states:

> An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities.[20]

In addition, NIST SP 800-53 Rev. 5, states: "The organization must protect the plan from unauthorized disclosure and modification."[21]

NIST SP 800-161, Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,* states:

> The purpose should outline the enterprise's high-level purpose for the strategy and implementation of the document to align with the purpose with the enterprise's mission, vision, and values. The SCRM plan should designate those responsible for the strategy and implementation template, as well as its key contributors.

This finding arose because OCIO did not thoroughly review NIST SP 800-161, Rev. 1, to ensure its SCRM policy included sufficient detail to allow for successful implementation. In addition, OCIO did not allocate the necessary time to develop robust policies.

The failure to enhance and implement SCRM policies and procedures could result in undetected weaknesses in supply chain elements and an increased risk of harm due to security measures being exploited from supply chain-related events.

We recommend that the CIO:

2. Review applicable NIST documentation and update the related SCRM policies and strategy accordingly while also ensuring leadership with SCRM roles and responsibilities perform a thorough review of the policy.

[20] NIST SP 800-53, Rev. 5, Control PM-30, SCRM Strategy
[21] NIST SP 800-53, Rev. 5, Control Supply Chain Risk Management (SR) – 2

PROTECT – CONFIGURATION MANAGEMENT

FINDING 4 – DEVIATIONS IN BASELINE CONFIGURATIONS NOT DOCUMENTED

For 7 of 12 IT Shared Services systems selected for testing, OCIO did not document, approve, or remediate deviations identified from the baseline for 31 of 32 servers, in accordance with the DOL's Operating System Baseline Creation SOP. Specifically, we noted the following:

- For System 1, we tested 2 servers and identified 153 undocumented deviations.
- For System 2, we tested 2 servers and identified 12 undocumented deviations.
- For System 3, we tested 8 servers and identified 272 undocumented deviations.
- For System 4, we tested 5 servers and identified 178 undocumented deviations.
- For System 5, we tested 10 servers and identified 147 undocumented deviations.
- For System 6, we tested 3 servers and identified 96 undocumented deviations.
- For System 7, we tested 1 server and identified 60 undocumented deviations.

Section 6.1 of the Operating System Baseline Creation SOP states:

> All existing baseline Operating System Baseline Configuration Documents (images) are reviewed on an annual basis. If any deviations are needed and conflict with the CSH, CPP, or other DOL Policy, the ISO/ISSO must submit a risk response request with input from ITOS.[22]

[22] See Appendix E for the abbreviations used in this excerpt.

The CPP, Volume 5, Section 2.6, states:

> The system owner or representative will establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using system-defined procedures. Additionally, the system owner or representative will monitor and control changes to the configuration settings in accordance with organizational policies and procedures.[23]

This CPP criteria was developed in accordance with Security Control CM-6 in NIST SP 800-53, Rev 5.

This finding occurred because OCIO management did not hold the personnel responsible for documenting deviations in accordance with the Operating System Baseline Creation SOP.

Failure to implement the process to approve deviations from established configuration settings led to an increased risk of unauthorized and undetected changes to the settings, which could result in a compromise of the integrity, confidentiality, and security of DOL's information systems.

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

- Implement a process for approving deviations from established configuration settings. (FY 2020 Recommendation 11)
- Develop and implement performance metrics for configuration management. (FY 2019 Recommendation 5)
- Enforce DOL requirements for implementing, auditing, testing, and documenting exceptions to baseline configurations. (FY 2021 Recommendation 4)

FINDING 5 – NON-KEV VULNERABILITIES NOT REMEDIATED WITHIN SPECIFIED TIMEFRAME

For 2 of 12 IT Shared Services systems selected for testing, OCIO did not remediate non-KEV high and critical vulnerabilities within the 60-day required

[23] DOL CPP, Volume 5: Configuration Management (CM) Standards and Procedures, Section 2.6: CM-6 Configuration Settings (January 2023)

timeframe, in accordance with the CPP. Specifically, 2 of 15 critical vulnerabilities and 3 of 15 high vulnerabilities were not remediated timely or documented and tracked within a POA&M.

For 1 of 2 IT Shared Services systems selected for external penetration and vulnerability testing, two medium vulnerabilities were identified that were not remediated timely or documented and tracked within a POA&M. For 1 of 2 IT Shared Services systems selected for external penetration and vulnerability testing, one low vulnerability was identified that was not remediated timely or documented and tracked within a POA&M.

The CPP, Volume 14, Section 2.5, states: "Agencies are required to remediate non-KEV critical, high, and moderate vulnerabilities within 60 days."[24]

OCIO management stated that this finding occurred because it did not have sufficient resources to mitigate all vulnerabilities within the defined timeframe. OCIO prioritizes remediating KEV vulnerabilities over non-KEV vulnerabilities, as they present a higher risk to information systems.

For the vulnerabilities identified through the external penetration testing, this finding occurred because the DOL Enterprise Security Operation Center team does not have visibility to identify potential risk on the external URLs tested. This contrasts with the selected systems development teams' visibility and allows potential threats to go unidentified.

Applying updated patches to mitigate software flaw vulnerabilities reduces the opportunities for exploitation, as patches correct security and functionality problems in software and firmware. The failure to apply patches appropriately and timely could lead to an increase of vulnerabilities, which in turn could result in a compromise of the integrity, confidentiality, and security of the agency's information systems.

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

- Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner. (FY 2019 Recommendation 8)

- Implement a centralized process to monitor vulnerabilities for information systems to ensure that each vulnerability is remediated within the

[24] DOL CPP, Volume 14: Risk Assessment (RA) Standards and Procedures, Section 2.5: RA-5 Vulnerability Monitoring and Scanning (January 2023)

timeframe defined by the Computer Security Handbook (CSH). (FY 2021 Recommendation 8)

- Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process. (FY 2020 Recommendation 12)

- 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 Common vulnerability and exposures. (FY 2019 Recommendation 7)

FINDING 6 – LACK OF STATIC APPLICATION VULNERABILITY SCANNING

For 1 of 12 IT Shared Services systems and 1 of 3 non-IT Shared Services systems selected for testing, static application scanning was not performed.

The CPP, Volume 14, Section 2.5, states: "OCIO will monitor and scan all systems for vulnerabilities in the system and hosted applications on an ongoing basis and when new vulnerabilities potentially affecting the system are identified and reported."[25] This criteria was developed in accordance with Security Control RA-5 in NIST SP 800-53, Rev 5.

For the one IT Shared Services system, the database supporting the system was running on an unsupported version of Oracle and was being phased out. For the one non-IT Shared Services system, we were informed that the DOL agency did not have sufficient resources to perform static application scanning on its IT systems.

The lack of static application scanning resulted in undetected vulnerabilities. A vulnerability that is not remediated could lead to the degradation of the system's integrity, availability, and confidentiality.

We did not provide a recommendation as the findings were previously identified by management and are tracked in a POA&M.

[25] DOL CPP, Volume 14: Risk Assessment (RA) Standards and Procedures, Section 2.5: RA-5 Vulnerability Monitoring and Scanning

PROTECT – IDENTITY AND ACCESS MANAGEMENT

FINDING 7 – LACK OF UPDATED RULES OF BEHAVIOR ACKNOWLEDGEMENT

For 1 of 12 IT Shared Services systems selected for testing, 6 of 15 nonprivileged users did not re-acknowledge the updated ROB, dated June 2022. Specifically, one nonprivileged user did not re-acknowledge the ROB until April 2023, four nonprivileged users did not re-acknowledge the ROB until May 2023, and one nonprivileged user did not re-acknowledge the updated ROB at all.

The CPP, Volume 12, Section 2.4, states: "The CIO or designee (for Enterprise Shared Services [ESS] agencies) or the agency head or designee, for non-ESS agencies, shall require individuals who have acknowledged a previous version of the ROB to read and re-acknowledge when the rules are revised or updated."[26] This criteria was developed in accordance with Security Control PL-4 in NIST SP 800-53, Rev 5.

This finding arose as OCIO did not develop and implement compliance review controls to ensure nonprivileged users were held accountable to acknowledge and sign the ROB when updated.

Failure to acknowledge and sign the updated ROB led to an increased risk that users were unaware of prohibited activities that would jeopardize the integrity, confidentiality, and availability of the information system.

We recommend that the CIO:

3. 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.

[26] DOL CPP, Volume 12: Planning Standards and Procedures, Section 2.4: PL-4: RoB (January 2023)

SUMMARY OF OCIO'S RESPONSE

OCIO generally concurred with all of KPMG's recommendations in the FY 2023 DOL FISMA Report. All recommendations identified have been remediated or plan to be remediated in FY 2024. OCIO will provide corrective action plans to address the recommendations for consideration for closure by the OIG. OCIO reinforced their commitment to cybersecurity and the ongoing nature of their IT cybersecurity portfolio improvement.

APPENDIX A: SCOPE, METHODOLOGY, AND CRITERIA

SCOPE

In accordance with FISMA, the objective of this performance audit was to determine the effectiveness of DOL's information security program. As such, we assessed relevant security controls and processes referenced in the five Cybersecurity Framework Function areas outlined in the FY 2023 IG FISMA Metrics. We responded to the FY 2023 IG FISMA Metrics and assessed the maturity levels on behalf of DOL OIG.

We also performed procedures to assess management's controls over ensuring the completeness and accuracy of the information used for the CIO FISMA Reporting to OMB for Quarter 2 of FY 2023. For a selection of metrics and an additional five systems, we performed procedures to assess the completeness and accuracy of the information that the OCIO reported for the Core IG ISCM metric related to ongoing information system assessments. We performed an external penetration test on two public facing URLs from 2 of 12 selected IT Shared Services systems. In addition, we followed up on the status of prior year recommendations.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2023 Core and Supplemental IG FISMA Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memoranda referenced in the reporting metrics; and the DOL CPP. The CPP was not released until January 2023; therefore, the DOL CSHs were utilized as criteria from October 2022 through December 2022. We reviewed the DOL information security program from a program-level perspective and then examined how each of the information systems selected for our testing implemented these policies and procedures for operating effectiveness.

We made a judgmental[27] 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, 2023. 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.

[27] 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.

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.

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

Tests of internal controls must be sufficiently extensive to provide reasonable assurance that the controls being tested operate 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 in the following paragraphs. Table 5 provides the frequency of control operation (population size) and the minimum sample size:

- *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 guidance to support the preliminary assessments of controls and conclude on the effectiveness of the controls.

- *Sample sizes where population < 5,000 items* – Per Financial Audit Manual 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 number of sample sizes (assuming zero exceptions), which are consistent with prior DOL FISMA performance audits (see Table 5).

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 Financial Audit Manual guidance

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 FY 2023 Core and Supplemental IG FISMA Metrics:

- We requested that 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 FY 2023 Core and Supplemental IG FISMA 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. FY 2023 introduced a calculated average scoring model. As part of this approach, FY 2023 Core and Supplemental IG FISMA Metris were averaged independently to determine a domain's maturity calculation. The calculated average scoring model is used for FY 2023. As part of this approach, Core Metrics and Supplemental Metrics have been averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. The overall score will average totals from each domain and be separated by Core Metrics and Supplemental Metrics. The calculated average was not automatically rounded as other data points were used to make a risk-based determination of the overall program.

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

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

- an inspection of the information security practices and policies established by the OCIO;

- an inspection of the information security practices, policies, and procedures in use across DOL;
- an inspection of artifacts to determine the design, implementation, and operating effectiveness of security controls at the program and system levels;
- the execution of an external penetration test on a selection of public facing DOL information systems;
- an inspection of OCIO's procedures to collect and report the information used to support DOL's Quarterly CIO FISMA Reporting to OMB;
- a comparison of information from the DOL agency data call workbooks to the information in the FISMA CIO Reporting to OMB for Quarter 2 of FY 2023; and
- an inspection of artifacts to corroborate information in the FISMA CIO Reporting to OMB for Quarter 2 of FY 2023 for a selection of DOL information systems.

We performed our fieldwork from January 3, 2023, through June 30, 2023. The penetration testing was performed as of June 21, 2023. All testing was performed through virtual meetings, walk-throughs, and observations with DOL representatives. Additionally, we held regular status meetings with DOL management.

CRITERIA

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines for use in the development and implementation of agencies' security programs. We used NIST SP 800-53, Rev. 5, in our assessment of relevant information security controls. We also utilized DOL's CPP, which outlines DOL's requirements for information security.

APPENDIX B: 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: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA
Digitally signed by GUNDEEP AHLUWALIA
Date: 2023.11.20 08:57:04 -05'00'

SUBJECT: Management Response to DRAFT REPORT – (Fiscal Year) FY 2023 FISMA DOL Information Security Report: Making Improvements Towards Meeting Management and Measurable, Report Number: 23-24-001-07-725

This memorandum responds to the above-referenced Draft Report – FY 2023 FISMA DOL Information Security Report: Making Improvements Towards Meeting Management and Measurable, Report Number: 23-24-001-07-725, issued November 3, 2023. Cybersecurity continues to be a top priority at the Department, and DOL leadership remains committed to continuously strengthening DOL's cybersecurity posture. DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve upon within the cybersecurity program.

Management generally concurs with the findings identified during the FY 2023 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 2024. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).

During FY 2023, DOL continued enhancing its cybersecurity program, including areas prioritized under Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" (May 12, 2021). For example, DOL continued working on enterprise-wide solutions to encrypt data-at-rest and in-transit as well as implementing multifactor authentication. DOL continued to partner with The Department of Homeland Security in the implementation of its Continuous Diagnostics and Mitigation (CDM) capability, Additionally, DOL leveraged funding from the Technology Modernization Fund to make progress in implementing a zero-trust solution to meet requirements of the Executive Order.

DOL accomplished the following cybersecurity results during FY 2023:

- During FY 2023 FISMA Audit, worked with OIG to close 38 OIG-issued prior year (PY) audit recommendations. During the FY 2023 FISMA Audit, worked with OIG to close 38 OIG-issued prior year (PY) audit recommendations. In addition, closure memos were received for 8 prior-year recommendations throughout FY 2023, for a total of 46 recommendations closed, reducing the number of open PY recommendations by more than 65 percent.
- Overhauled the Computer Security Handbook (CSH) and published the Cybersecurity Capability Portfolio (CPP) to establish NIST SP 800-53 Rev. 5 compliant policies, streamlining 500 pages of requirements into 190 pages.
- Offered awareness training sessions to assist with policy implementation and transition support for various topics (i.e., Cloud and Third-Party Systems, Risk-Based Decisions).

- 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.
- Enhanced DOL's Information Security Continuous Monitoring (ISCM) capability by implementing performance metrics across the three risk management tiers to measure the effectiveness of the security controls, increase oversight, and provide senior leaders centralized visibility to drive risk-based decision-making.
- Improved the FISMA OIG-determined maturity level for 11 of the 20 core metrics tested, compared to FY 2022, with 50 percent of the metrics rated as *Effective* (Level 4 or Level 5).
- Boosted the FISMA OIG-determined maturity level for 10 out of 20 non-core metrics tested, an increase from FY 2021, with 70 percent of the metrics achieving an Effective rating (Level 4 or Level 5).

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

- Implement enterprise-wide solutions for data encryption and multifactor authentication.
- Continue the monitoring and protection of critical software and the maturing of capabilities for supply chain risk management.
- Enhance DOL's enterprise log management capability in accordance with OMB M-21-31.
- Execute the roadmap for implementation of a zero-trust architecture.
- Implement Security Operations Center (SOC) enhancements that will allow the Department to anticipate and mitigate risk and stay ahead of the evolving threat landscape. Finalize the implementation of data loss prevention tools and alerts.
- Complete transition of DOL FISMA reportable systems to NIST 800-53 Rev. Complete transition of DOL FISMA reportable systems to NIST SP 800-53 Rev.

As demonstrated in the enclosed FISMA report, DOL has implemented a robust cybersecurity program and plans to further improve its cybersecurity 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 the responsible party 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
Karl Hellmann, Deputy Chief Information Security Officer
Muhammad Butt, Division Director, Information Security Policy & Planning (DISSP)

APPENDIX C: FINDING REFERENCE

Finding No.	Function	Domain	Issued Finding/Factual Accuracy No.
1	Identify	Risk Management	FA OCIO-RM-01
2	Identify	Risk Management	NoF FISMA-23-03
3	Identify	Supply Chain Risk Management	NoF FISMA-23-01
4	Protect	Configuration Management	FA system1-CM-01
5	Protect	Configuration Management	FA system2-CM-02
6	Protect	Configuration Management	FA system2-CM-01 FA system3-CM-01
7	Protect	Identity and Access Management	NoF FISMA-23-02

APPENDIX D: STATUS OF PRIOR YEAR RECOMMENDATIONS

As part of the FY 2023 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 the recommendations had been sufficiently implemented and there were no related issues identified during our FY 2023 testing, we determined the recommendation was closed. If there was evidence the recommendations had been only partially implemented or not implemented at all, we determined the recommendations remained open. Based on our testing, we determined 38 recommendations were closed and 31 recommendations remained open.

Table 5: Progress DOL Has Made in Closing Prior Year Recommendations

Related Domain	Report Year	Prior Year Recommendation	Status of Recommendation
RM	2011	Assess and take appropriate measures to ensure reports of lost, missing, or stolen sensitive IT assets have not resulted in loss of sensitive (PII) information in accordance with US-CERT and DOL Information Breach Policy and Procedures.	**Open**
RM	2011	Perform a full inventory of DOL's IT assets that is accurate and complete, including an update of the information into a viable inventory management system.	**Open**
RM	2011	Consolidate all inventory systems throughout DOL to eliminate duplication, realize cost savings, and strengthen inventory.	**Open**

RM	2011	Integrate a reliable electronic procurement system with a viable inventory system along with the financial systems.	**Open**
RM	2011	Perform required reviews of program agencies' inventory practices and procedures to ensure full participation in the inventory process across the Department and compliance with Federal information system requirements.	**Open**
RM	2011	Develop policies for disposal of sensitive information technology assets that presently lack coherent policy.	**Open**
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	2018	Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies that have been communicated to DOL management.	**Closed**
RM	2019	Verify that annual assessments of third-party providers, including cloud service providers, are formally documented, reviewed, and signed by appropriate levels of management.	**Closed**
RM	2019	Implement technologies for both DOL and the Bureau of Labor Statistics to detect and prevent unauthorized hardware and software from	**Closed**

		connecting to the local DOL network.	
RM	2019	Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner.	**Open**
RM	2019	Conduct a complete inventory of DOL IT assets (i.e., computers, hard drives, tablets, mobile phones, etc.).	**Open**
RM	2019	Assess the adequacy of existing security measures relating to DOL IT assets.	**Open**
RM	2020	Complete, approve, and implement its Enterprise Architecture and related artifacts.	**Closed**
RM	2020	Provide training to responsible personnel over the third-party continuous monitoring review checklist.	**Closed**
RM	2020	Validate that the classification of DOL systems is in accordance with policy, and that system interconnections are appropriately documented within its inventory.	**Closed**
RM	2021	Enforce DOL requirements for authorizing connections and effective implementation of Interconnection Service Agreements.	**Closed**
RM	2021	Implement changes in oversight that enforce DOL requirements for the performance of the monthly continuous monitoring checklist for Cloud Service	**Closed**

		Providers in accordance with the DOL CSH.	
RM	2021	Establish an MOU or other agreement between the OCIO and all departmental agencies to establish and state the roles and responsibilities of IT between each set of respective agencies.	**Open**
RM	2021	Codify the policies and procedures that define IT governance and key supporting IT elements.	**Open**
RM	2021	Reassess the incorporation of BLS and OCFO as part of IT Shared Services within 2021 and document the reasoning for the decision reached.	**Open**
RM	2021	Ensure the CIO is a lead member with voting rights of DOL's executive strategy and management boards and committees including but not limited to the Management Review Board (MRB), ESS Governance Board, COVID-19 Coordination team, and Enterprise Risk Management Council (ERMC).	**Open**
RM	2021	Reorganize the CIO position to have a direct reporting relationship to the Deputy Secretary and independent of Assistant Secretary for Administration and Management (ASAM).	**Open**
RM	2021	Develop and implement a centralized process or mechanism for tracking monthly reviews of Cloud Service Providers.	**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	2022	Develop and implement policies and procedures to update DOL's system repository based on a defined frequency.	**Closed**
RM	2022	Verify if systems have been appropriately authorized in accordance with DOL's policy.	**Closed**
CM	2019	Design and implement controls and policies to formally perform and document the periodic review of baseline configuration scans across DOL servers and databases.	**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.	**Open**
CM	2020	Enforce DOL policies and procedures regarding separation of duties so developers do not possess the ability to migrate changes to production.	**Closed**
CM	2020	In accordance with DOL Change Management Plan and NIST SP 800-55, Rev. 1, develop, define, implement, and monitor change management key performance indicators that	**Closed**

		align DOL's goals and objectives.	
CM	2020	Enforce its security baseline polices with DOL's CSPs and develop a security configuration checklist for the CSPs.	**Closed**
CM	2020	Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process.	**Open**
CM	2020	Implement a process for approving deviations from established configuration settings.	**Open**
CM	2021	Ensure DOL maintains a complete and accurate inventory of its hardware and software assets.	**Closed**
CM	2021	Enhance the management oversight by OCIO to enforce DOL requirements for the performance of annual reviews of unsecure functions, ports, protocols, and services.	**Closed**
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.	**Open**

CM	2021	Implement a centralized process to monitor vulnerabilities for information systems to ensure that each vulnerability is remediated within the CSH defined timeframe.	**Open**
CM	2022	Implement proper quality control to ensure change management processes are being performed for all systems and equipment on the DOL network.	**Open**
DPP	2019	Implement data encryption configurations and solutions at the server level for data at rest for sensitive information (PII).	**Open**
IAM	2019	Develop and implement access control performance metrics.	**Closed**
IAM	2019	Finalize the implementation of the access control technologies.	**Open**
IAM	2019	Design and implement controls to perform and document a periodic review of audit logs that report privileged user activity.	**Closed**
IAM	2019	Coordinate efforts among the DOL agencies to design and implement procedures and controls to address account management in key financial feeder systems.	**Open**
IAM	2019	Monitor the agencies' progress to ensure that established procedures and controls are operating effectively and maintained.	**Open**

IAM	2020	Implement a process for periodic review or monitoring of PIV Exemptions to ensure the process is operating effectively.	**Closed**
IAM	2020	Implement policies and procedures regarding user access reviews for tenants that reside on the Platform as a Service (PaaS) in accordance with requirements outlined in the DOL CSH.	**Closed**
IAM	2020	Provide additional resources to support the security requirements and a training over the application user access review process, as documented in the DOL CSH.	**Closed**
IAM	2020	Document the responsibilities of control activities for tenants that reside on the PaaS through policies and procedures that include user activity reviews in accordance with requirements outlined in the DOL policy.	**Closed**
IAM	2020	Provide training over the application user activity review process.	**Closed**
IAM	2020	Reinforce the PIV Exemption approval process through training.	**Closed**
IAM	2021	Implement a system or tool to retain rules of behavior acknowledgements, access authorizations, other required documentation for authorized system access, and periodic user access reviews. OCIO should monitor this system or tool to ensure each FISMA-reportable system is compliant with the DOL CSH account management	**Closed**

		policies.	
IAM	2021	Strengthen the OCIO controls to monitor system owners to ensure they implement appropriate audit logging controls in accordance with the CSH.	**Closed**
ISCM	2018	Develop and implement performance metrics that will be used to manage and measure the effectiveness of the DOL information security program.	**Closed**
ISCM	2019	Develop and implement contingency planning performance metrics.	**Closed**
ISCM	2020	Develop sufficiently defined quantitative and qualitative metrics that provide meaningful indications of security status and trend analysis at all risk management tiers.	**Closed**
ISCM	2021	Enhance the OCIO oversight of the DOL ISCM strategy at the enterprise and system level and ensure DOL systems have an implemented system-level continuous monitoring strategy.	**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**

IR	2022	Develop Departmental policies and procedures that require all DOL agencies to perform data exfiltration tests to identify gaps in its data exfiltration and network defense.	**Closed**
IR	2022	Implement data loss prevention tools and alerts based on the results of agencies' data exfiltration tests.	**Open**
IR	2022	Enhance incident response activity training to emphasize the importance of submitting required incidents to the US-CERT within the 1-hour timeframe.	**Closed**
IR	2022	Implement an automated mechanism to report incidents to the US-CERT within the 1-hour timeframe.	**Closed**
CP	2020	Validate that systems have received either the appropriate classification or risk waiver that would exempt the system from specific security requirements.	**Closed**
CP	2020	Monitor contingency plan testing and exercises through examination of after-action reviews.	**Closed**
CP	2021	Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of contingency plan tests.	**Closed**
CP	2021	Enhance the OCIO monitoring of the completion of the required annual training by individuals with CP responsibilities.	**Closed**

CP	2021	Enhance the OCIO monitoring and oversight of system owners to complete BIAs.	**Open**

APPENDIX E: ACRONYMS AND ABBREVIATIONS

Acronym / Abbreviation	Definition
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ASAM	Assistant Secretary for Administration and Management
BIA	Business Impact Analysis
BLS	Bureau of Labor Statistics
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	Department of Homeland Security
DOL	Department of Labor
DPP	Data Protection and Privacy
EO	Executive Order
ERMC	Enterprise Risk Management Council
ESS	Enterprise Shared Services
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IAM	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISO	Information Security Officer
ISSO	Information System Security Officer
IT	Information Technology
ITOS	Information Technology Operations and Services
KEV	Know Exploited Vulnerability
KPMG	KPMG LLP

Acronym / Abbreviation	Definition
MOU	Memorandum of Understanding
MRB	Management Review Board
NIST	National Institute of Standards and Technology
NoF	Notice of Finding
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PaaS	Platform as a Service
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
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
URL	Uniform Resource Locators
US-CERT	United States Computer Emergency Readiness Team

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