U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2022 FISMA DOL INFORMATION SECURITY REPORT: DOL'S INFORMATION SECURITY PROGRAM NOT REMAINING CURRENT WITH SECURITY REQUIREMENTS

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

Carolyn Hantz
Assistant Inspector General for Audit

DATE ISSUED: FEBRUARY 10, 2023
REPORT NUMBER: 23-23-001-07-725

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

BRIEFLY…

FY 2022 FISMA DOL INFORMATION SECURITY REPORT: DOL'S INFORMATION SECURITY PROGRAM NOT REMAINING CURRENT WITH SECURITY REQUIREMENTS

February 10, 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) 2022 information security program for the period October 1, 2021, through June 30, 2022. 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 the security controls and targeted vulnerability assessments.

WHAT OIG FOUND

KPMG reported nine findings for DOL's information security program within five of five Cybersecurity Framework Functions and six of nine FISMA Metric Domains, which resulted in the U.S. Department of Homeland Security's FISMA reporting system determining DOL's information security program was not effective for FY 2022.

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 four of the five Cybersecurity Framework Functions: Identify, Protect, Detect, and Recover. A security program is only considered effective if the majority of the Cybersecurity Framework Functions are rated at least Managed and Measurable (Level 4).

The information security program's scores showed some decline from FY 2021, which was caused by DOL's delayed implementation of National Institute of Standards and Technology Special Publication 800-53, Revision 5. KPMG noted further deficiencies in the performance of security control assessments, account management controls, and contingency planning controls.

Based on the issues identified by KPMG, we continue to be concerned about the remaining corrections needed in the Office of Chief Information Officer's oversight and accountability over DOL's information security control environment.

WHAT OIG RECOMMENDED

KPMG made eight recommendations to strengthen DOL's information security program.

READ THE FULL REPORT

https://www.oig.dol.gov/public/reports/oa/2023/23-23-001-07-725.pdf

TABLE OF CONTENTS

U.S. Department of Labor

Office of Inspector General
Washington, DC 20210

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) 2022 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 (GAGAS).

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, 2021, through June 30, 2022. 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 a data exfiltration assessment on three DOL general support networks. Additional details regarding the scope of the independent audit are included in KPMG's report.

RESULTS

KPMG identified and reported nine findings for DOL's information security program. The findings were identified in all five of the FISMA Cybersecurity Framework Functions and in six of the nine FISMA Metric Domains, which resulted in the U.S. Department of Homeland Security's FISMA reporting system (CyberScope) determining DOL's information security program was not effective for FY 2022.

A security program is considered effective if the majority of the FY 2022 Core IG Metrics reported in CyberScope are at least Managed and Measurable (Level 4); however, KPMG found weaknesses that demonstrated the information security program had not achieved a maturity rating of Managed and Measurable (Level 4) in four of the five FISMA Cybersecurity Framework Functions: Identify, Protect, Detect, and Recover.

KPMG also found DOL's information security program did not fully adhere to applicable FISMA requirements, Office of Management and Budget (OMB) policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines. For example, DOL's entity-wide and system-level security policies and procedures 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 performance of security control assessments, account management controls, and contingency planning controls.

KPMG made eight recommendations related to control deficiencies. The Chief Information Officer (CIO) noted in his January 23, 2023, response that his office will provide details regarding each of the audit's findings and recommendations in a later management decision response. KPMG also evaluated the implementation of recommendations from prior FISMA reports. Out of 20 previously open recommendations related to FY 2018 and FY 2019 FISMA evaluations as well as FY 2020 and FY 2021 FISMA performance audits, KPMG determined DOL has successfully closed five recommendations.

In reviewing the results from KPMG's testing, we are concerned the CIO inability to bring DOL into compliance with NIST SP 800-53, Rev. 5; controls impact all metric areas and was a cause for the decline in scores from FY 2021. The implementation of NIST SP 800-53, Rev. 5, was due to be completed for new systems at the start of FY 2021 and existing systems by the start of FY 2022. Instead, DOL is currently aiming to have these controls in place by the third quarter of FY 2023, a significant delay that impacts all areas of DOL's information security program. Our concern is heightened about this issue given the CIO has not documented the risk nor has the CIO accepted the risk of DOL information security controls not being compliant with NIST SP 800-53, Rev. 5. With so many control areas at risk, the confidentiality, integrity, and availably of DOL's systems are at risk.

We reviewed the Office of the Chief Information Officer's (OCIO) management comments to these findings and our concerns, as well as KPMG's response. We note that the OCIO did not provide additional evidence. Therefore, based on our oversight of KPMG's work during the audit, we determined the results remain factually correct and fully supported.

We appreciate the cooperation and courtesies DOL and the OCIO personnel extended us during this audit.

Carolyn R. Hantz

Carolyn R. Hantz
Assistant Inspector General
for Audit

CONTRACTOR PERFORMANCE AUDIT REPORT

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

Independent Audit on the Effectiveness of the U.S. Department of Labor's Information Security Program and Practices Report – Fiscal Year 2022

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 March 1, 2022, through August 31, 2022, and our scope focused the period of October 1, 2021, through June 30, 2022.

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) 2022 Core Inspector General (IG) FISMA Metrics.[1] We responded to the FY 2022 Core IG FISMA Metrics and assessed the maturity levels on behalf of the DOL Office of Inspector General (OIG). In addition, we identified non-Core IG FISMA Metrics[2] to determine the

[1] OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*
[2] *FY 2021 IG FISMA Reporting Metrics*

effectiveness of DOL's information security program. We also followed up on the status of prior-year recommendations.

Based on the maturity levels calculated in CyberScope,[3] we determined DOL's information security program was not effective as it did not fully adhere to applicable FISMA requirements, Office of Management and Budget (OMB) policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines. A security program is considered effective if the majority of the FY 2022 Core IG FISMA Metrics are at least Managed and Measurable (Level 4). Table 1 depicts the maturity levels for the five Cybersecurity Framework Functions.

Table 1: Maturity Levels for Cybersecurity Framework Functions

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

Source: FY 22 Inspector General Section Report for the Department of Labor

During FY 2022, we tested security controls at the entity level and for a selection of 20 systems. In addition, we performed a data exfiltration assessment on three DOL general support networks. We identified nine findings for DOL's information security program. The findings were identified in five of the five FISMA Cybersecurity Framework Functions and in six of the nine FISMA Metric Domains. In accordance with our procedures, we considered the identified findings when we assessed the maturity levels for each of the FY 2022 Core IG FISMA Metrics, which were input into the CyberScope reporting tool. Based on those inputs, CyberScope calculated and output a program assessment of "not effective" for DOL's information security program.

DOL's entity-wide and system-level security policies and procedures have not been updated to comply with NIST Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Federal Information System and*

[3] CyberScope, operated by the Department of Homeland Security on behalf of OMB, is a web-based application designed to streamline information technology (IT) 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.

Organization (NIST SP 800-53, Rev. 5). Additionally, we noted deficiencies in the performance of security control assessments, account management controls, and contingency planning controls.

In response to these control deficiencies, we made eight recommendations related to strengthening DOL's information security program. However, we did not make recommendations for two control deficiencies as they correspond to open prior-year recommendations. We recommend 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 implement robust monitoring capabilities to continually assess the security state of its systems to include a process to hold these agencies accountable for identified compliance gaps.

We also evaluated the implementation of recommendations from prior FISMA reports. Out of 20 previously open recommendations related to FY 2018 and FY 2019 FISMA evaluations as well as FY 2020 and FY 2021 FISMA performance audits, we determined DOL has successfully closed five recommendations.

KPMG LLP cautions 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, DOL OIG, the Department of Homeland Security, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

February 9, 2023

BACKGROUND

KPMG LLP (KPMG) performed the Fiscal Year (FY) 2022 independent Federal Information Security Modernization Act of 2014 (FISMA) performance audit under contract with Department of Labor (DOL) as a performance audit in accordance with generally accepted government auditing standard (GAGAS). The DOL Office of Inspector General (OIG) monitored our work to ensure 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 of 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 many workplace activities for about 10 million workplaces and 150 million workers.

PROGRAM OVERVIEW

The DOL Office of the Chief Information Officer (OCIO) operates within the Office of the Assistant Secretary for Administration and Management and as a customer service organization dedicated to providing information technology (IT) solutions and leadership to advance its mission. OCIO has four strategic goals in support of DOL's mission:

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

- **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.

- **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.

- **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 primary objectives of the DOL information security effort are ensuring:

1. The confidentiality of sensitive information processed by, stored in, and moved through information systems and applications belonging to DOL

2. The integrity of the DOL information, such that decisions and actions are taken based upon the data processed by, stored in, and moved through DOL information systems, can be made with the assurance that the data has not been manipulated, the data is not subject to repudiation, and the source of changes to data can be determined as best as possible

3. The availability of DOL information systems and applications during routine operations and in crisis situations to support the DOL mission

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

On December 17, 2002, the President signed FISMA into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The act's purposes include providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets as well as providing a mechanism for improved oversight of federal agency information security programs.

FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment (1) included the reestablishment of the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

FISMA requires senior agency officials to provide information security for the information and information systems that support the operations and assets under their control, including 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.

FISMA INSPECTOR GENERAL METRICS AND REPORTING

The Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, DHS, and the Federal Chief Information Officers and Chief Information Security Officers councils, developed the FY 2022 Core Inspector General (IG) Metrics[4] based on the five Cybersecurity Framework Functions outlined in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[5] (herein referred to as the Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.[6]

[4] OMB's *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*

[5] In its *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, 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 decisions, addressing threats, and improving by learning from previous activities.

[6] EO 13636, *Improving Critical Infrastructure Cybersecurity*, was issued on February 12, 2013, which 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.

The FY 2022 Core IG FISMA Metrics were chosen based on alignment with Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (specifically the Multifactor Authentication section and the Encryption and Software Supply Chain Security & Critical Software section),[7] 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)
- *Improving the Federal Governments' Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31)
- *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01)

In addition, OMB's *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (M-22-05),[8] adjusted the timeline for the IG evaluation. Specifically, M-22-05 required that a core group of metrics be evaluated annually, and the remainder of the metrics be evaluated on a 2-year cycle, agreed to by CIGIE, the Chief Information Security Officer Council, OMB, and the Cybersecurity and Infrastructure Security Agency.

The FY 2022 Core IG FISMA Metrics use a capability maturity model developed by OMB, DHS, CIGIE, and other stakeholders for the nine FISMA Metric Domains. Table 2 outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domains.

[7] Executive Order 14028, *Improving the Nation's Cybersecurity*

[8] OMB's Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (M-22-05)

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 2021 Inspector General 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 simple majority, where the most frequent level (mode) for the questions was the Domain rating. When responses are entered into the CyberScope reporting tool,[9] 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. A security

[9] CyberScope, operated by the Department of Homeland Security on behalf of OMB, is a web-based application designed to streamline information technology (IT) security reporting for federal agencies.

program is considered effective if a simple majority[10] of the FY 2022 Core IG FISMA Metrics are 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 2021 Inspector General 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.

[10] Simple Majority, defined as “The most frequent level (i.e., mode) across the questions” from the *FY 2021 Inspector General Reporting Metrics*

RESULTS

Based on the maturity levels calculated in CyberScope, we determined DOL's information security program was not effective for the five Cybersecurity Framework Functions and nine FISMA Metric Domains 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 majority of the FY 2022 Core 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: Maturity Levels for Cybersecurity Framework Functions and FISMA Metric Domains

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	Defined (Level 2)
Respond – IR	Managed and Measurable (Level 4)
Recover – CP	Consistently Implemented (Level 3)

Source: FY 22 Inspector General Section Report for the Department of Labor

During FY 2022, we tested security controls at the entity level and for a selection of 20 systems. We also performed additional procedures on relevant controls related to the Authorization to Operate, CM, Plans of Action and Milestones (POA&M), and system and data backup and conducted a data exfiltration testing on three DOL networks.

We identified nine findings, which were identified in all of the five FISMA Cybersecurity Functions and in six of the nine FISMA Metric Domains. We also evaluated the implementation of recommendations from prior FISMA reports. Out of 20 previously open recommendations related to FY 2018 and FY 2019 FISMA evaluations and FY 2020 and FY 2021 FISMA performance audits, we determined DOL has successfully closed 5 recommendations. See Appendix E for the complete list of these prior-year findings and recommendations.

During our testing for the FISMA Metric Domains, OCIO did not provide requested documentation in a timely manner to demonstrate performance of its control activities in the applicable FISMA Metric Domains including RM, IAM, DPP, and CP. Specifically, OCIO did not provide:

- Evidence related to system audit logs, access agreements, baseline configuration, patch management, Interconnection Service Agreements, backups, and configuration settings for a selection of servers for 1 of 13 IT Shared Services[11] systems selected for testing;

- Rules of Behavior documentation for 1 of 13 IT Shared Services systems;

- Evidence to demonstrate data encryption of personally identifiable information (PII); and

- A Customer Responsibility Matrix for 1 of 5 cloud systems selected for testing.

As reported by OCIO, this was due to competing priorities and lack of resources. However, we received enough supporting documentation for these impacted areas to assess the maturity levels of the applicable FY 2022 Core IG FISMA Metrics. Therefore, we were still able to conclude on the corresponding controls and determine the effectiveness of DOL's information security program.

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 DOL's *Identify* Function at the Consistently Implemented (Level 3) maturity level. As described in detail below, we found OCIO did not update entity-wide security policies and procedures to be compliant with NIST Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Federal Information System and Organization* (NIST SP 800-53, Rev. 5). We

[11] The DOL Enterprise Shared Services is a consolidation and centralization of core administrative functions such as procurement, personnel and physical security, Human Resources Services, and IT. IT Shared Services refers to the services and systems that have been brought under the OCIO umbrella for centralization and oversight. Non-IT Shared services refers to systems that are outside of that boundary and are controlled by their individual Departments, such as the OIG, Job Corps, and Bureau of Labor Statistics.

also noted system-level security plans, policies, and procedures were not updated to conform to NIST SP 800-53, Rev. 5. In addition, OCIO did not finalize its SCRM strategies, policies, and procedures to manage supply chain risks. OCIO is in the process of enhancing its risk management policies and procedures; however, our testing identified issues in its implementation of RM and SCRM security controls.

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 these documented RM decisions.

Based on the results of our performance audit procedures, we assessed DOL's RM FISMA Metric Domain as Consistently Implemented (Level 3). We determined OCIO implemented policies and procedures to maintain a complete and accurate inventory of its major information systems, hardware devices, and software. 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. However, OCIO did not track hardware and software assets specific to major information systems and did not monitor software and hardware assets for non-IT Shared Services systems selected for testing.

We found OCIO developed and implemented processes for authorizing information systems, performing risk assessments, and tracking and monitoring POA&Ms. OCIO also utilized the Continuous Diagnostics and Mitigation (CDM) program to provide enterprise IT security reports and dashboards; however, it did not use automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to DOL systems and data.

Further, OCIO uses the Cybersecurity Assessment Management (CSAM) tool as the primary source for obtaining risk data and maintaining the official system inventory. DOL stakeholders used these processes to identify, manage, and track cybersecurity risks in an official Cybersecurity Risk Register, which is integrated into DOL's Enterprise Risk Register. While the Cybersecurity Risk Register included system POA&Ms and risk responses, it did not include risks that OCIO considered from the operation and use of its information systems and the variability of environments that exists within DOL. Additionally, OCIO did not aggregate and normalize cybersecurity risks based on defined risk categories and criteria.

OCIO developed a Cybersecurity Policy Portfolio (CPP) Developmental Schedule that outlined their plan to update security policies and procedures at the departmental level and at the system level to comply with NIST SP 800-53, Rev. 5. The plan consisted of five implementation phases, which began with updating the CPPs to reflect changes and ended with a phased approach to transition the NIST SP 800-53, Rev. 5, controls to all DOL systems by the end of third quarter of FY 2023. However, OCIO did not comply with their Enterprise Risk Management Framework Strategy to create a risk response and POA&M to track the risk acceptance. We determined this was a pervasive issue as each FISMA Metric Domain has applicable NIST SP 800-53, Rev. 5, criteria.

We determined that OCIO did not define a frequency in their policies for updating CSAM to ensure DOL's system inventory is accurate.

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 and helps to ensure appropriate contractual requirements are included for acquisitions.

Based on the results of our performance audit procedures, we assessed DOL's SCRM FISMA Metric Domain as Ad Hoc (Level 1). OCIO performed reviews of products, system components, systems, and services as a part of the acquisition process to identify cybersecurity issues and concerns. However, it was still in the process of developing the SCRM policy to identify requirements for managing supply chain risks and accounts in compliance with NIST SP 800-53, Rev. 5. Additionally, OCIO did not consistently monitor third-party providers, as associated prior-year recommendations remained unimplemented.

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 at the Consistently Implemented (Level 3) maturity level. While we found DOL developed and implemented policies, procedures, and guidance for CM, IAM, DPP, and ST, our testing found issues with the implementation and operating effectiveness of security controls in the CM, IAM, and DPP 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 Defined (Level 2). While we noted OCIO developed and implemented CM policies and procedures, during our testing we found issues in the implementation and operating effectiveness of CM controls related to prior-year findings regarding secure configurations and vulnerability and patch management, which have not been remediated.

OCIO used tools to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for its IT Shared Services information system components connected to its network; however, OCIO did not continuously monitor security configurations for its non-IT Shared Services information system components. Further, OCIO did not employ automation to manage DOL's system components. Specifically, OCIO did not utilize system CM tools to measure the settings of operating systems and applications connected to the DOL network.

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, scanning results, and the remediation process. Additionally, OCIO did not centrally manage static application security testing vulnerability scanning.

OCIO did not consistently retain evidence of approval, testing, and security impact analyses prior to the implementation of changes for one non-IT Shared Services system selected for testing.

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 screening, issuing and maintaining user credentials, and managing logical and physical access privileges. These activities collectively are referred to as Identity, Credential, and Access Management.

Based on the results of our procedures, we assessed DOL’s IAM FISMA Metric Domain as 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 related to prior-year findings that require sufficient corrective actions and control deficiencies identified in this year’s performance audit.

OCIO continued to implement new capabilities to automate the account management of information system nonprivileged accounts. OCIO was in the process of integrating tools to automate user provisioning and deprovisioning[12] and to manage privileged identities for all privileged users. However, OCIO did not fully employ automated mechanisms to support the management of information system privileged accounts, including account review and recertification for its information systems. We noted DOL did not ensure controls were in place to perform privileged user reviews and privileged user activity audit log reviews for one IT Shared Services system selected for testing.

OCIO met federal targets for the implementation of the identity proofing and authentication processes for nonprivileged and privileged users. Additionally, in accordance with EO 14028, *Improving the Nation’s Cybersecurit*y, OCIO reported 97 percent of its FISMA-reportable systems were covered by Multifactor Authentication as of March 14, 2022. However, OCIO did not maintain a list of accepted external authenticators for its systems, in accordance with NIST SP 800-53, Rev. 5. Also, OCIO was implementing a phased approach to complete a Digital Identity Risk Assessment (DIRA) for all systems that reside on the DOL network, but a DIRA was not performed on all systems selected for testing.

[12] Provisioning is the process of creating and configuring a user account to be used by an end user. Deprovisioning is the process of removing access rights for a user account.

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 PII increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource*, 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 within their agency, EO 13719, *Establishment of the Federal Privacy Council*, requires agency heads to designate a senior agency official for privacy who has agency-wide responsibility and accountability for the agency's privacy program.

Based on the results of our procedures, we assessed DOL's DPP FISMA Metric Domain as Consistently Implemented (Level 3). OCIO had a Privacy Program in place for the protection of PII and other sensitive data; however, we determined there were significant changes to the relevant controls in NIST SP 800-53, Rev. 5, that were not addressed in the program. We determined DOL effectively sanitized media prior to disposal.

As in previous years, 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, *Improving the Nation's Cybersecurity*, OCIO reported 81 percent of FISMA-reportable systems had implemented encryption for data-at-rest and 82 percent of the systems implemented encryption for data-in-transit as of March 14, 2022.

We determined OCIO performed data exfiltration tests to analyze the performance of its enhanced network defenses for IT Shared Services systems selected for testing, but OCIO did not ensure non-IT Shared Services systems were performing data exfiltration tests.

We performed data exfiltration testing and determined security controls, including the data loss prevention tools that prevent data exfiltration and enhance network defenses, were not fully implemented across the DOL network. Further, non-IT Shared Services agencies did not configure relevant systems to send alerts to their Computer Security Incident Response Team to initiate required action as a response to the data exfiltration testing.

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 Consistently Implemented (Level 3). 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, and updating training based on feedback received from users and evolving threats and risks. However, OCIO did not create plans to address all identified skill gaps in its workforce assessment.

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. As a result of our procedures, we assessed DOL's *Detect* Function and the aligned ISCM FISMA Metric Domain as Defined (Level 2).

Congress established the CDM program to provide agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. OCIO was in the process of updating its current integration of the CDM dashboard to comply with the DHS dashboard. However, the CDM dashboard was not in production.

OCIO did not develop system-level continuous monitoring strategies for DOL systems in accordance with NIST SP 800-53, Rev. 5. OCIO did not fully transition to ongoing control and system authorization for DOL systems. OCIO did not define and implement time-driven triggers to identify the frequency for which Authorizing Officials (AO) were required to review security-related information to determine if the risk of continued system operation remained acceptable. Further, OCIO did not develop and implement automated measures to support near real-time risk management for its information systems. The output should be specific, measurable, actionable, relevant, and timely to determine the effectiveness of each control and provide value to determine the system's security and privacy posture.

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 IR policies, procedures, plans, strategies, and technologies. It also monitored and analyzed the effectiveness of its incident response policies, procedures, plans, strategies, and technologies through weekly reports that capture IR activities. OCIO utilized multiple advanced tools to support the IR processes. These tools fed into DOL's Security Information and Event Management tool to give a centralized view of the incidents. Further, OCIO utilized profiling techniques to maintain a comprehensive baseline of network operations and expected data flows for users and systems.

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). While we noted that OCIO developed and implemented CP policies and procedures, our testing found deficiencies in the operational effectiveness of its CP security controls. We also found OCIO needed to develop meaningful qualitative and quantitative metrics and monitor them to determine the effectiveness of its *Recover* Function.

OCIO did not consistently perform contingency plan tests and Business Impact Analyses (BIA) in accordance with the DOL CSH for two IT Shared Services systems selected for testing.

AUDIT FINDINGS AND RECOMMENDATIONS

IDENTIFY – RISK MANAGEMENT

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

DOL did not update its information security and privacy policies and procedures for the Department and its systems to be compliant with NIST SP 800-53, Rev. 5, as required by OMB Circular A-130, *Managing Information as a Strategic Resource*. OCIO did not complete a formal risk waiver, nor did it establish a POA&M to address this deficiency.

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. Also, for legacy information systems, agencies are expected to meet the requirements of, and be in compliance with, NIST standards and guidelines within 1 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.

In addition, the DOL Enterprise Cybersecurity Risk Management Strategy, Section 3, states that the risk must be entered in the CSAM tool with an associated POA&M. The risk response should be submitted using the Risk Response Request template, to include the risk acceptance recommended by the Chief Information Security Officer. Per the strategy, the risk response will also be accepted by the AO as appropriate.

This finding occurred due to the level of effort required to implement the controls throughout the cybersecurity program as well as OCIO not holding management accountable for following the departmental risk management policies and procedures over accepting risk.

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

We recommend that the Chief Information Officer (CIO):

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

FINDING 2 – INVENTORY NOT UPDATED

OCIO did not define a frequency for updating its official system inventory in CSAM. Therefore, OCIO did not update CSAM for new systems implemented in FY 2022 in a timely manner. For a selection of 12 new IT Shared Services systems and non-IT Shared Services systems, CSAM was not updated to reflect the operational status for 1 IT Shared Services system. Specifically, the system's go-live date was March 31, 2022, but the system was not updated to an "Operational" state in CSAM until May 12, 2022.

Control Program Management-5 System Inventory in NIST SP 800-53, Rev. 5, requires organizations to develop and update their inventory of systems on a defined frequency. However, OCIO did not develop policies and procedures to update DOL's inventory of systems to accurately reflect DOL systems' operational statuses in a timely manner.

Organizations rely on accurate information in their inventory to perform strategic planning activities, to fulfill daily operational decisions, and to meet federal reporting guidelines. When the system inventory is not complete and accurate, there can be increased risks that systems are not included in DOL's information continuous monitoring process and may not have appropriate security controls in place.

We recommend that the CIO:

2. Develop and implement policies and procedures to update DOL's system repository based on a defined frequency.

PROTECT – CONFIGURATION MANAGEMENT

FINDING 3 – LACK OF APPROPRIATE CONFIGURATION CHANGE MANAGEMENT

We selected one non-IT Shared Services system for testing. For two of four Solaris operating system changes tested, the support team could not provide evidence of approval, testing, and security impact analysis, as required by the DOL CSH.

The DOL CSH, *Volume 5, Configuration Management Policy, Procedure and Standards,* Section 3.1.2, states the configuration change control process includes the systematic proposal, justification, implementation, testing, review, and disposition of changes to the system. Additionally, prior to implementation, DOL is responsible for analyzing changes to the information system for potential security impacts.

This finding arose because the servers in question were scheduled to be decommissioned. The system's management was not holding personnel accountable for performing change management activities.

The purpose of documenting the approval, testing, and impact analysis of configuration changes is to ensure the changes are appropriate to implement into the production environment with limited security impact to the information system. When configuration changes are not tracked or monitored, there is an increased risk of unauthorized system and data changes, as well as the loss of the confidentiality, integrity, and availability of DOL's information systems. Also, a change may be implemented with resulting security ramifications that impact the effectiveness of other controls or create new unmitigated security risks.

We recommend that the CIO:

3. Implement proper quality control to ensure change management processes are being performed for all systems and equipment on the DOL network.

PROTECT – IDENTITY AND ACCESS MANAGEMENT

FINDING 4 – USER ACCOUNT MANAGEMENT CONTROLS WERE NOT FOLLOWED

For 1 of 13 IT Shared Services systems selected for testing, OCIO did not access its privileged user accounts for 9 months, until May 2022, which was not within the semiannual frequency requirement defined in the DOL CSH. In addition, OCIO did not have a control in place to review privileged user activity for indications of inappropriate or unusual activity on a monthly basis, as required by the DOL CSH.

The DOL CSH, *Volume 1, Access Control Protection Policy, Procedure and Standards,* Section 3.1.1, states information system accounts should be reviewed every six months to verify and validate (recertify) that all active privileged and nonprivileged user accounts are still required based on user needs and rights.

The DOL CSH, *Volume 3, Audit and Accountability Policy, Procedure and Standards*, Section 3.2.1, states that management is required to review and analyze the system's records at least monthly for indications of inappropriate or unusual activity and report any findings to designated agency officials. Additionally, in NIST SP 800-53, Rev. 5, the control "Access Control-2 – Account Management" requires accounts to be reviewed in compliance with the organization-defined frequency. Also in NIST SP 800-53, Rev. 5, the control "Audit and Accountability-6 – Audit Review, Analysis, and Reporting" requires system audit records to be reviewed and analyzed for indications of organization-defined unusual activity at a defined frequency.

This finding arose due to OCIO not retaining key personnel or properly planning for the transfer of personnel. OCIO was unable to ensure individuals were equipped with the knowledge and ability to develop policies and procedures to perform the review of privileged users and the review of privileged-user activity.

When biannual access reviews are not completed for privileged user accounts, there can be an increased risk of unauthorized access to and modification of production data and computing resources.

We did not provide a recommendation as the finding is related to the following unimplemented prior-year recommendations that OCIO has not addressed:

- Design and implement controls to perform and document a periodic review of audit logs that report privileged user activity.
- Provide additional resources to support the security requirements and a training over the application user access review process, as documented in the DOL CSH.
- Provide training over the application user activity review process.
- Implement a control to retain rules of behavior acknowledgments, access authorizations, other required documentation for authorized system access, and periodic user access reviews.
- Monitor this control to ensure each FISMA-reportable system is in compliance with the DOL CSH account management policies.

PROTECT – DATA PROTECTION AND PRIVACY

FINDING 5 – DATA EXFILTRATION TESTING FAILURES

For one IT Shared Services system and two non-IT Shared Services systems, security controls to prevent data exfiltration and enhance network defenses were not fully implemented. Fictitious sensitive data files sent from DOL via email were inappropriately received by the remote KPMG server:

- For the two non-IT Shared Services systems, five of six emails containing sensitive data files were received by the KPMG server.
- For one IT Shared Services system, two of seven emails containing sensitive data files were received by the KPMG server.

Additionally, for two of two Non-IT Shared Services systems, alerts were not configured to generate as a response to the data exfiltration test. OCIO also did not ensure the two non-IT Shared Services systems were performing data exfiltration testing.

In NIST SP 800-53, Rev. 5, the control “System and Communications Protection-7 – Boundary Protection” requires that an organization monitor and control communication at external managed interfaces to the system and at key internal managed interfaces with the system. Also, the control “System and

Information Integrity-7 – Software, Firmware, and Information Integrity" requires that organizations employ integrity verification tools to detect unauthorized changes to software, firmware, and information.

Metric #37 of the *FY 2022 Core IG FISMA Metrics Evaluation Guide*[13]—which asks, "[t]o what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses?"—requires the following for the maturity level of Consistently Implemented (Level 3):

> The organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked.

This finding occurred due to the lack of requirement per Departmental policy for OCIO's bureaus and offices to perform data exfiltration testing. Furthermore, this led to a lack of awareness of gaps within systems' data exfiltration and network defenses.

Without proper data exfiltration controls or data loss prevention tools, sensitive information may be shared outside of the DOL network. This led to an increased risk of improper handling of PII/Protected Health Information, disclosure of sensitive departmental information, and unauthorized users accessing sensitive data. Additionally, without alerts configured and monitoring in place, security personnel will not be notified and therefore, unable to take appropriate action in a timely manner.

We recommend that the CIO:

4. 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

5. Implement data loss prevention tools and alerts based on the results of agencies' data exfiltration tests.

[13] *FY 2022 Core IG FISMA Metrics Evaluation Guide*

DETECT – INFORMATION SECURITY CONTINUOUS MONITORING

FINDING 6 – SECURITY CONTROL ASSESSMENT NOT PERFORMED PROPERLY

For one IT Shared Services system selected for testing, OCIO did not include the FY 2022 Security Control Assessment Plan's (SCAP) "Control IP-04 – Compliant Management," as required by OCIO Security's Annual Security Assessment (ASA) Plan.

The DOL CSH, *Volume 6, Contingency Planning Policy, Procedure, and Standards,* Section 3.2.1, states ASAs are required to be conducted in a manner compliant with the OCIO Security Center's guidance. The control "Assessment, Authorization, and Monitoring-2 – Control Assessments," in NIST SP 800-53, Rev. 5, requires controls in the system and its environment of operation to be assessed at the organization-defined frequency.

This finding occurred because management did not effectively maintain an accurate System Security Plan. As the SCAP is developed based on the information in the System Security Plan, the system's SCAP did not include one hybrid control required to be tested.

The purpose of a security control assessment is to identify deficiencies, provide essential information needed to make risk-based decisions as part of security authorization processes, and ensure compliance to vulnerability mitigation procedures. When controls are not tested there is a risk that threats and vulnerabilities are being overlooked that could increase the risks to the information system and data.

We did not provide a recommendation as the finding is related to the following unimplemented prior-year recommendation that OCIO has not addressed:

- 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.

FINDING 7 – SYSTEM NOT AUTHORIZED PROPERLY

For one IT Shared Services system selected for testing, the individual who was deputy CIO signed the Authorization to Operate instead of the AO, who was the CIO.

The DOL CSH*, Volume 4, Security Assessment and Authorization Policy, Procedure, and Standards,* Section 3.1.6, states the AO must authorize in writing the information system used for processing DOL data before commencing operations. This responsibility cannot be delegated. Also, the control "Control Assessment-6 – Authorization," in NIST SP 800-53, Rev. 5, requires that the AO for the system authorizes the system before commencing operations.

This finding occurred because the CIO was out on leave. Since the AO responsibilities are assigned to an individual and not title, DOL should have followed the standards outlined in the CSH, Volume 4, *Security Assessment and Authorization Policy, Procedure, and Standards,* Section 3.1.6, which states that the AO must authorize the information system in writing for processing DOL data before commencing operations. This responsibility cannot be delegated.

When the assigned AO does not authorize an information system, the AO could be unaware of the residual risks of the information system that could impact the information system and data.

We recommend that the CIO:

6. Verify if systems have been appropriately authorized in accordance with DOL's policy.

RESPOND – INCIDENT RESPONSE

FINDING 8 – INCIDENT NOTIFICATION NOT REPORTED TIMELY

For a selection of 15 incidents, OCIO Security Center did not timely report 1 incident that impacted the confidentiality of DOL's IT environment to the US-CERT within the 1-hour timeframe established by US-CERT Federal Incident Notification Guidelines and the DOL CSH. DOL indicated that the incident was ultimately reported to the US-CERT 4 hours and 8 minutes late.

The DOL CSH*, Volume 8, Incident Response Policy, Procedure, and Standards,* Section 1.5.3, states the DOL Computer Security Incident Response Team will officially confirm the incident status and report all true incidents impacting confidentiality, integrity, or availability to the US-CERT within 1 hour of the final determination. The US-CERT Federal Incident Notification Guidelines state agencies must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian or Executive Branch agency is potentially compromised, to the US-CERT with the required data elements, as well as any other available information, within 1 hour of being identified by the agency's top-level Computer Security Incident Response Team. Additionally, in NIST SP 800-53, Rev. 5, the control "Incident Response-6 – Incident Reporting" requires personnel to report suspected incidents to the IR capability and defined authorities within the defined period.

This finding occurred because an analyst failed to click "submit" when they completed the security incident ticket to submit to US-CERT. Although this exception occurred, DOL's maturity level for IR was assessed as Level 4: Managed and Measurable.

The untimely reporting can increase risk to the confidentiality, integrity, and availability of DOL information systems and data. Reporting incidents in a timely manner to the US-CERT can expedite the initial notification to uncover associated vulnerabilities and inform risk assessments. Further, it can improve situational awareness of cybersecurity events affecting the government.

We recommend that the CIO:

7. Enhance incident response activity training to emphasize the importance of submitting required incidents to the US-CERT within the 1-hour timeframe

8. Implement an automated mechanism to report incidents to the US-CERT within the 1-hour timeframe.

RECOVER – CONTINGENCY PLANNING

FINDING 9 – CONTINGENCY TESTING NOT COMPLETED

DOL's contingency planning controls were not consistently followed, as described below:

1. The approved BIA for 1 of 13 IT Shared Services systems selected for testing did not include a Maximum Tolerable Downtime, Recovery Point Objective, or Time Response Severity Level.

2. For 1 of 13 IT Shared Services systems selected for testing, management did not perform the contingency plan test within the required annual frequency established by the DOL CSH.

The DOL CSH, *Volume 6, Contingency Planning Policy, Procedure, and Standards,* Section 2.1, requires that a BIA be completed as part of DOL's information system contingency planning process. The BIA identifies and prioritizes system components as they correlate to the organization's mission and business process(s), essential function(s), and interdependencies. Based on this information, the agency must characterize the consequences of a disruption or system unavailability. The contingency plan must be tested at least annually, per the DOL CSH, *Volume 6, Contingency Planning Policy, Procedure, and Standards,* Section 3.2.1. Also, in NIST SP 800-53, Rev. 5, the control "Contingency Planning-2 – Contingency Plan," requires that contingency plans provide recovery objectives, restoration priorities, and metrics. The control "Contingency Planning-4 – Contingency Plan Testing" requires the contingency plan to be tested per the organization-defined frequency to determine the effectiveness of the plan.

This finding arose due to the improper monitoring of the system to ensure the completion of the required annual contingency plan test and competing priorities for new personnel. Furthermore, OCIO did not properly plan for the transfer of personnel.

Not performing an annual contingency plan test could impact DOL's response to restoring essential operations.

We did not provide a recommendation as the finding is related to the following unimplemented prior-year recommendations that OCIO has not addressed:

- Enhance the OCIO monitoring and oversight of system owners to complete BIAs
- Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of contingency plan tests.

CONCLUSIONS

Based on the calculations performed in CyberScope, DOL's information security program was assessed as not effective because a majority of the Cybersecurity Framework Function areas outlined in the FY 2022 Core IG FISMA Metrics were rated Consistently Implemented (Level 3) or Defined (Level 2). Specifically, four of five Cybersecurity Framework Function areas were rated below Managed and Measurable (Level 4). Therefore, we assessed DOL's information security program and practices for its information systems as not effective.

We issued nine findings within each of the five Cybersecurity Framework Functions and six of the nine FISMA Metric Domains and made eight recommendations related to these findings to strengthen DOL's information security program if effectively addressed by management. We did not make a recommendation for two findings as they correspond to open prior-year recommendations. The recurring findings indicate the root cause of the issues have not been addressed. Further, the findings resulted from a lack of proper quality control in the monitoring of DOL's information systems. The root causes that led to each of the findings identified as part of this performance audit may contribute to control findings for other systems outside the scope of this audit.

We recommend that the CIO consider applying these recommendations to the entire universe of systems for improving and progressing the maturity of the DOL information security program. Further, we recommend that the CIO implement robust monitoring capabilities to continually assess the security state of these systems to include a process to hold these agencies accountable for identified compliance gaps.

In a written response, the CIO partially concurred with three of our findings and recommendations, concurred with four of our findings, and did not concur with four of our findings. The CIO did not provide planned corrective actions that were responsive to the intent of our recommendations.[14] CIO's response to the draft report is included in its entirety in Appendix C.

[14] We issued 11 Notice of Findings (NOFs) to management that were consolidated into 9 findings in the report with 8 recommendations. The counting of the CIO's concurrences, partial concurrences, and non-concurrences is based on the 11 NOFs. For finding 6 in the report, we did not provide a recommendation as it is related to an unimplemented prior-year recommendation.

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 2022 Core IG FISMA Metrics. We responded to the FY 2022 Core IG FISMA Metrics and assessed the maturity levels on behalf of DOL OIG.

In addition, we performed additional procedures on relevant controls related to change management, POA&Ms, security training, system backups, and data exfiltration. We also performed data exfiltration testing on three DOL networks. We also followed up on the status of prior-year recommendations.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2022 Core IG FISMA Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memorandums referenced in the reporting metrics; and the DOL CSH. 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 selection of 20 information systems (16 federal and 4 contractor information systems) from a total population of 71 information systems as of March 1, 2022. We selected 13 IT Shared Services federal systems and 3 non-IT Shared Services federal systems. Our testing also included DOL-wide information security controls.

METHODOLOGY

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

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 testwork where the population size exceeded 5,000 items, we selected a sample of 45 items (assuming zero exceptions) per Government Accountability Office *Financial Audit Manual* (FAM) guidance to support the preliminary assessments of controls and conclude on the effectiveness of the controls.

- *Sample sizes where population < 5,000 items* – Per FAM guidance, for populations containing less than or equal to 5,000 items (i.e., testing of daily, weekly, monthly, quarterly controls, or the size of the population), we used the minimum 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/ 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 2022 Core 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.

- 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 assessed the maturity at Level 3 for the questions with responses indicating control failures.

- For metrics determined to be at Maturity Level 4, we performed further procedures leveraging Maturity Level 5 (Optimized) 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.

Per the results of our test procedures, we input the maturity level for each of the FY 2022 Core IG FISMA Metrics into the CyberScope reporting tool, which calculated the Cybersecurity Framework Function maturity levels based on the mode of the FISMA Metric Domain levels. The simple majority of the component Cybersecurity Function scores was used to calculate each Cybersecurity Domain’s maturity level.

Our procedures included the following 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 a data exfiltration assessment on the DOL network

We performed our fieldwork from March 1, 2022, through August 31, 2022. Due to the ongoing COVID-19 pandemic, all testing was performed remotely through virtual meetings, walk-throughs, and observations with DOL representatives.

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. Federal agencies were required to update their security policies and procedures to comply with NIST SP 800-53, Rev. 5*,* as it superseded NIST SP 800-53, Rev. 4, on September 23, 2021. As such, we used NIST SP 800-53, Rev. 5, in our assessment of relevant information security controls. We also utilized DOL's CSH, which outlines DOL's requirements for information security.

APPENDIX B: KPMG RESPONSE TO CIO'S RESPONSE TO THE REPORT

We acknowledge the response provided by the DOL CIO to the findings identified during the DOL Fiscal Year (FY) 2022 FISMA performance audit. We performed a thorough analysis of management's response and provide the following additional information. To facilitate tracking between the CIO's component comments that comprise the overall response, we included the same bold type labels (e.g., "Accuracy") in our response that the CIO used.

We used a risk-based approach for the FY 2022 performance audit. Our approach considered information provided by DOL management, such as the status of prior year findings, management's self-assessment, inquires; reviewing the DOL CSH and SSPs for the selected information systems; system selections based on FIPS-199 ratings, the last time the information system was tested, system type, and if the system was a high-value asset; the questions associated with the OMB FY 2022 Core IG Metrics; and OMB's associated evaluation guide. Our approach to assessing the information security program was based on the criteria associated with relevant metric questions and DOL's own policies. These inputs were used to develop our performance audit plan and procedures. Please refer to the Appendix A for details related to the FY 2022 methodology and approach.

While the CIO stated that he did not concur with all the findings identified during the performance audit, the CIO did not provide any additional, compelling evidence to refute the findings and did not identify mitigating controls for consideration. In prior years, we were provided additional information and evidence for consideration during the finding vetting process, which at times, would mitigate a finding. The CIO and other DOL OCIO representatives have only provided us with verbal explanations stating that they do not believe that we should report the findings.

Accuracy: The CIO stated the report incorrectly interprets DOL policy resulting in unwarranted findings and provided the specific example of the improper authorization of an information system. The CIO stated that the Deputy CIO was acting on behalf of the CIO and, as such, said action was not a delegation of responsibility. We respectfully disagree with this position and consider the CIO's tacit acceptance of the Deputy CIO's issuance of the authorization in question to be an in-substance delegation of responsibility. For the tested information system, the CIO (the person who holds this position) is the designated AO (by name and not position), and the Deputy CIO did not have formal authority to authorize the information system. According to the DOL CSH Volume 4: Security

Assessment and Authorization Policy, Procedure and Standards, Version 1.1, dated November 2021, Section 3.1.6, states "that the responsibility of Authorizing Official cannot be delegated." Additionally, NIST SP 800-37, Revision (Rev.) 2, Risk Management Framework for Information Systems and Organizations states, "The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document." OMB Circular A-130 establishes that the AO is responsible and accountable for the risks associated with the information system. In this instance, DOL should have performed risk management activities, such as recording this as a POA&M; formally accepted the risk that an individual without proper authority authorized the system; or had the Deputy CIO formally designated as the AO for the system.

Relevance: The CIO stated the report based certain findings on prior-year open recommendations that were not material to the FY 2022 performance audit; however, DOL CIO's response mischaracterized the reliance on open prior-year findings as it relates to this year's ratings. The prior-year SCRM recommendation did not impact the rating for FY 2022. The overall SCRM FISMA Metric Domain was assessed at a Level 1, Ad Hoc, maturity rating because the SCRM policy was in draft during the FY 2022 performance audit period and was not formally authorized and implemented. We determined that the prior-year recommendation that DOL OCIO provide training to conduct effective reviews of third-party systems was not closed. Further, as a result of current-year testing, we determined that, although DOL OCIO provided training to personnel responsible for conducting effective third-party system reviews, such personnel did not complete reviews in a timely manner according to the DOL CSH. As a result, we did not consider the training provided to be effective, and we determined that the prior-year recommendation remained open.

Impact: The CIO stated that our finding related to DOL's noncompliance with NIST SP 800-53, Rev. 5, did not pose any significant risk to DOL. DOL has not integrated Rev. 5 controls into its ISCM program. NIST added the new control requirements in Rev. 5 based on evolving cyber threats to provide safeguards and countermeasures to protect high-value assets. We noted the changes made to the privacy controls in NIST SP 800-53, Rev 5 and evaluated the DOL CSH and privacy program for compliance. We confirmed that DOL enterprise information security policies were not in compliance with NIST SP 800-53, Rev. 5. Furthermore, as part of our system-level testing (based on the NIST controls referenced in the metric questions), we performed procedures to assess whether the NIST SP 800-53, Rev. 5, controls were implemented and operating effectively. We determined that management did not implement these controls for the selected systems. For example, DOL did not develop system-level continuous monitoring strategies and did not update its identification and authentication controls. The final version of NIST SP 800-53, Rev. 5, was published in September 2020, and, according to OMB Circular A-130, implementation of the new controls required by NIST SP 800-53, Rev. 5, was required by September 2021. We inquired of the OCIO whether DOL had documented NIST SP 800-53, Rev. 5, noncompliance as a POA&M and were informed that no POA&M had been created. The findings cited in DOL CIO's response were associated with privacy controls that we identified as undergoing significant changes because of the transition from NIST SP 800-53 Rev. 4 to NIST SP 800-53 Rev. 5.

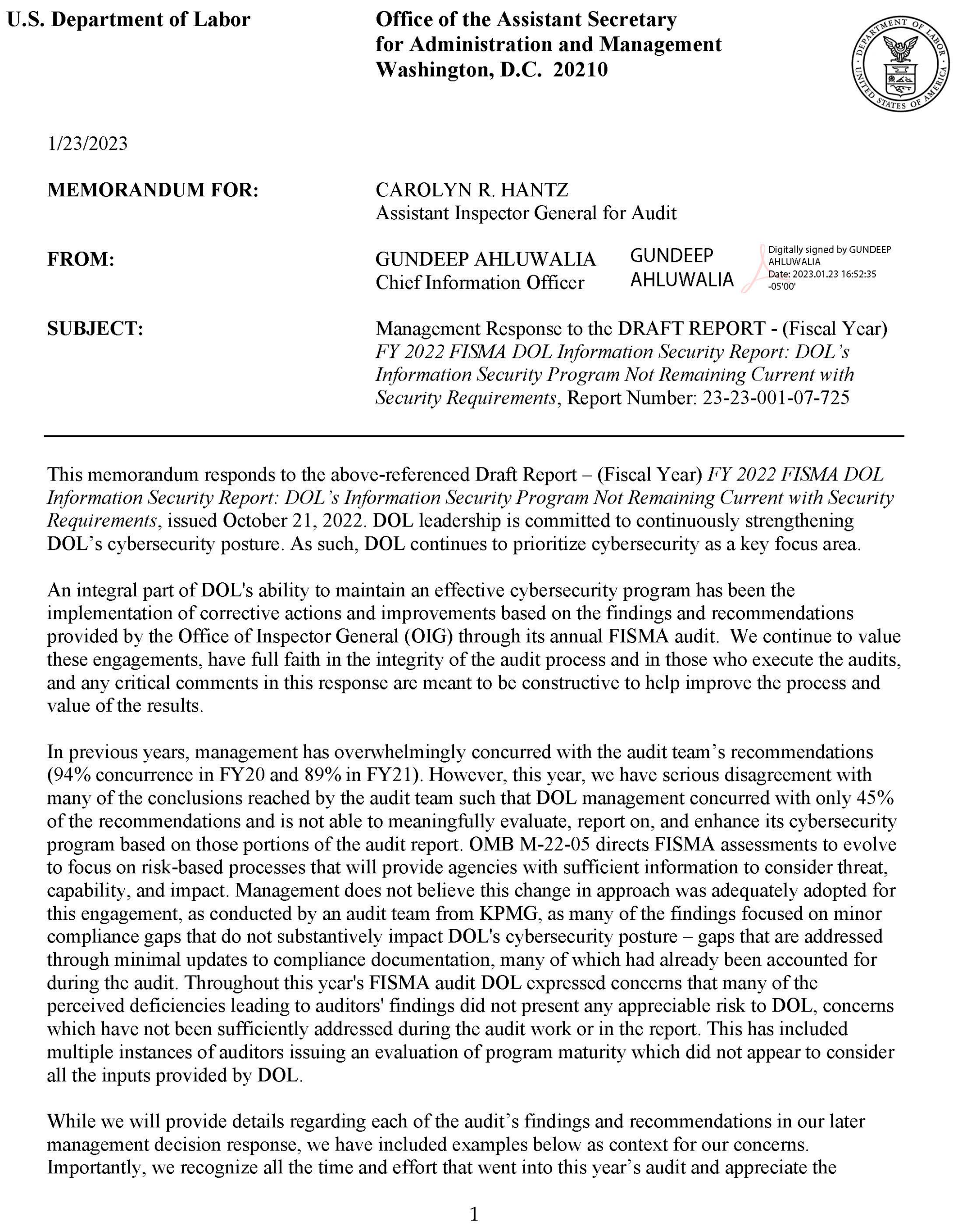
Risk: The CIO stated in its response that the findings identified in the report were inconsistent with the actual risk environment and specifically stated a "key" finding in the report was that a single security control assessment was not performed properly. While this finding was documented in the report and considered in our determination of the overall rating of the ISCM FISMA Metric Domain, it was not the sole driver of such. We reported additional findings associated with DOL's ISCM program, which included the lack of system ISCM plans (repeat finding from prior years), the lack of time-driven or event-driven triggers that should prompt an immediate review of security and privacy information by the AO for authorization in accordance with ongoing authorization, and the improper authorization of an information system. These findings represent instances in which DOL failed to consistently implement ISCM programmatic requirements that would allow them to identify, monitor and mitigate related threats and security control weaknesses, all of which contributed to the Level 2, Defined, maturity level for the ISCM FISMA Metric Domain.

Further, the CIO stated that "...findings did not present any appreciable risk…" We reported these findings to management based on the criteria used for the engagement which we included in Appendix A. On an individual basis, these findings did not impact the overall maturity levels assessed for the Cybersecurity Functions and FISMA Metric Domains calculated in CyberScope. Rather, we determined that DOL's information security program was ineffective based on the collective evidence gathered through audit procedures, new and open findings, and our assessment of DOL's information system security program based on the FISMA maturity model.

Risk: The CIO stated the finding regarding the untimely submission of incidents to United States Computer Emergency Response Team presented no risk to the system or the Department. Our methodology requires that we report findings identified during testing. We considered facts and circumstances in assessing relevant risk and, as such, we assessed the Incident Response Domain as Level 4, Managed and Measurable. We requested supporting documentation evidencing that DOL OCIO management performed a thorough root-cause analysis of factors contributing to the finding; however, we did not receive supporting documentation detailing the root cause. Therefore, we performed our own analysis and issued the recommendation to enhance incident response training.

We considered the points identified by the CIO regarding its progress to sustain cybersecurity maturity across all FISMA domains as a part of our testing. While DOL CIO noted areas of continued progress and tools that were being implemented, we base our procedures on the state of DOL's information security program (tools, people, and processes) during the period defined in the report. All evidence that was provided by DOL was taken into consideration during our testing and related maturity level ratings assigned. As such, we did not modify our findings and recommendations based on DOL CIO's response.

APPENDIX C: CIO'S RESPONSE TO THE REPORT



U.S. Department of Labor

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

1/23/2023

MEMORANDUM FOR: CAROLYN R. HANTZ
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA
Digitally signed by GUNDEEP AHLUWALIA
Date: 2023.01.23 16:52:35 -05'00'

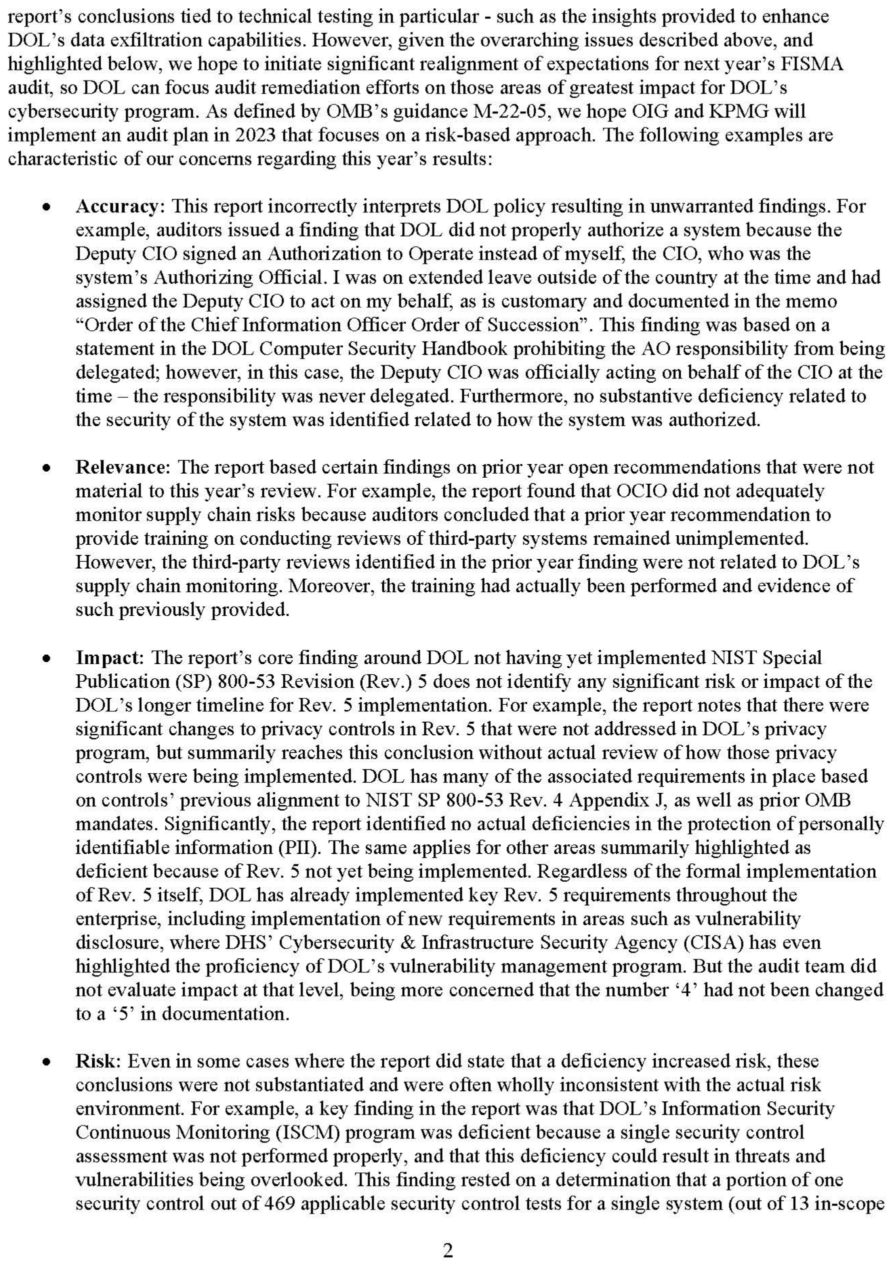
SUBJECT: Management Response to the DRAFT REPORT - (Fiscal Year) *FY 2022 FISMA DOL Information Security Report: DOL's Information Security Program Not Remaining Current with Security Requirements*, Report Number: 23-23-001-07-725

This memorandum responds to the above-referenced Draft Report – (Fiscal Year) *FY 2022 FISMA DOL Information Security Report: DOL's Information Security Program Not Remaining Current with Security Requirements*, issued October 21, 2022. DOL leadership is committed to continuously strengthening DOL's cybersecurity posture. As such, DOL continues to prioritize cybersecurity as a key focus area.

An integral part of DOL's ability to maintain an effective cybersecurity program has been the implementation of corrective actions and improvements based on the findings and recommendations provided by the Office of Inspector General (OIG) through its annual FISMA audit. We continue to value these engagements, have full faith in the integrity of the audit process and in those who execute the audits, and any critical comments in this response are meant to be constructive to help improve the process and value of the results.

In previous years, management has overwhelmingly concurred with the audit team's recommendations (94% concurrence in FY20 and 89% in FY21). However, this year, we have serious disagreement with many of the conclusions reached by the audit team such that DOL management concurred with only 45% of the recommendations and is not able to meaningfully evaluate, report on, and enhance its cybersecurity program based on those portions of the audit report. OMB M-22-05 directs FISMA assessments to evolve to focus on risk-based processes that will provide agencies with sufficient information to consider threat, capability, and impact. Management does not believe this change in approach was adequately adopted for this engagement, as conducted by an audit team from KPMG, as many of the findings focused on minor compliance gaps that do not substantively impact DOL's cybersecurity posture – gaps that are addressed through minimal updates to compliance documentation, many of which had already been accounted for during the audit. Throughout this year's FISMA audit DOL expressed concerns that many of the perceived deficiencies leading to auditors' findings did not present any appreciable risk to DOL, concerns which have not been sufficiently addressed during the audit work or in the report. This has included multiple instances of auditors issuing an evaluation of program maturity which did not appear to consider all the inputs provided by DOL.

While we will provide details regarding each of the audit's findings and recommendations in our later management decision response, we have included examples below as context for our concerns. Importantly, we recognize all the time and effort that went into this year's audit and appreciate the



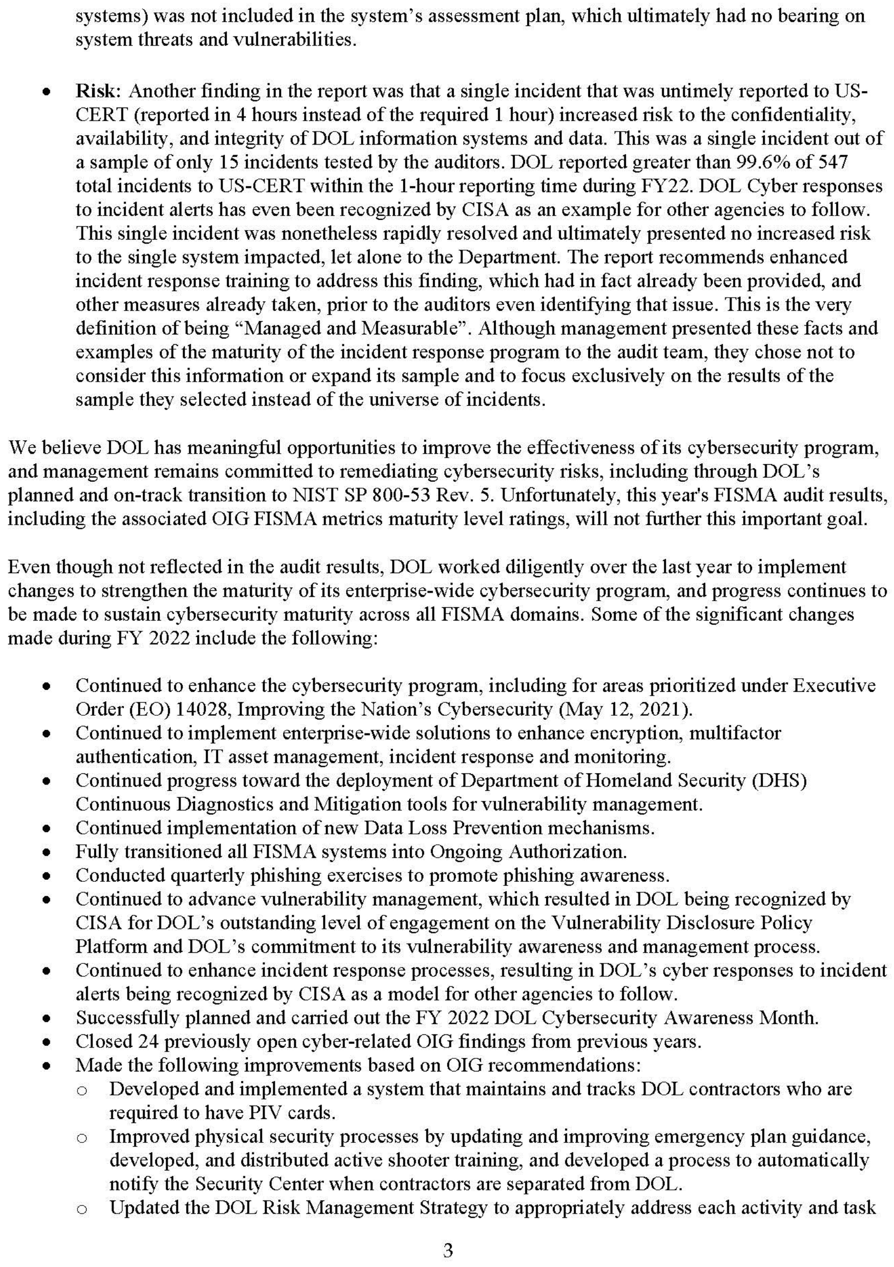
report's conclusions tied to technical testing in particular - such as the insights provided to enhance DOL's data exfiltration capabilities. However, given the overarching issues described above, and highlighted below, we hope to initiate significant realignment of expectations for next year's FISMA audit, so DOL can focus audit remediation efforts on those areas of greatest impact for DOL's cybersecurity program. As defined by OMB's guidance M-22-05, we hope OIG and KPMG will implement an audit plan in 2023 that focuses on a risk-based approach. The following examples are characteristic of our concerns regarding this year's results:

- **Accuracy:** This report incorrectly interprets DOL policy resulting in unwarranted findings. For example, auditors issued a finding that DOL did not properly authorize a system because the Deputy CIO signed an Authorization to Operate instead of myself, the CIO, who was the system's Authorizing Official. I was on extended leave outside of the country at the time and had assigned the Deputy CIO to act on my behalf, as is customary and documented in the memo "Order of the Chief Information Officer Order of Succession". This finding was based on a statement in the DOL Computer Security Handbook prohibiting the AO responsibility from being delegated; however, in this case, the Deputy CIO was officially acting on behalf of the CIO at the time – the responsibility was never delegated. Furthermore, no substantive deficiency related to the security of the system was identified related to how the system was authorized.

- **Relevance:** The report based certain findings on prior year open recommendations that were not material to this year's review. For example, the report found that OCIO did not adequately monitor supply chain risks because auditors concluded that a prior year recommendation to provide training on conducting reviews of third-party systems remained unimplemented. However, the third-party reviews identified in the prior year finding were not related to DOL's supply chain monitoring. Moreover, the training had actually been performed and evidence of such previously provided.

- **Impact:** The report's core finding around DOL not having yet implemented NIST Special Publication (SP) 800-53 Revision (Rev.) 5 does not identify any significant risk or impact of the DOL's longer timeline for Rev. 5 implementation. For example, the report notes that there were significant changes to privacy controls in Rev. 5 that were not addressed in DOL's privacy program, but summarily reaches this conclusion without actual review of how those privacy controls were being implemented. DOL has many of the associated requirements in place based on controls' previous alignment to NIST SP 800-53 Rev. 4 Appendix J, as well as prior OMB mandates. Significantly, the report identified no actual deficiencies in the protection of personally identifiable information (PII). The same applies for other areas summarily highlighted as deficient because of Rev. 5 not yet being implemented. Regardless of the formal implementation of Rev. 5 itself, DOL has already implemented key Rev. 5 requirements throughout the enterprise, including implementation of new requirements in areas such as vulnerability disclosure, where DHS' Cybersecurity & Infrastructure Security Agency (CISA) has even highlighted the proficiency of DOL's vulnerability management program. But the audit team did not evaluate impact at that level, being more concerned that the number '4' had not been changed to a '5' in documentation.

- **Risk:** Even in some cases where the report did state that a deficiency increased risk, these conclusions were not substantiated and were often wholly inconsistent with the actual risk environment. For example, a key finding in the report was that DOL's Information Security Continuous Monitoring (ISCM) program was deficient because a single security control assessment was not performed properly, and that this deficiency could result in threats and vulnerabilities being overlooked. This finding rested on a determination that a portion of one security control out of 469 applicable security control tests for a single system (out of 13 in-scope



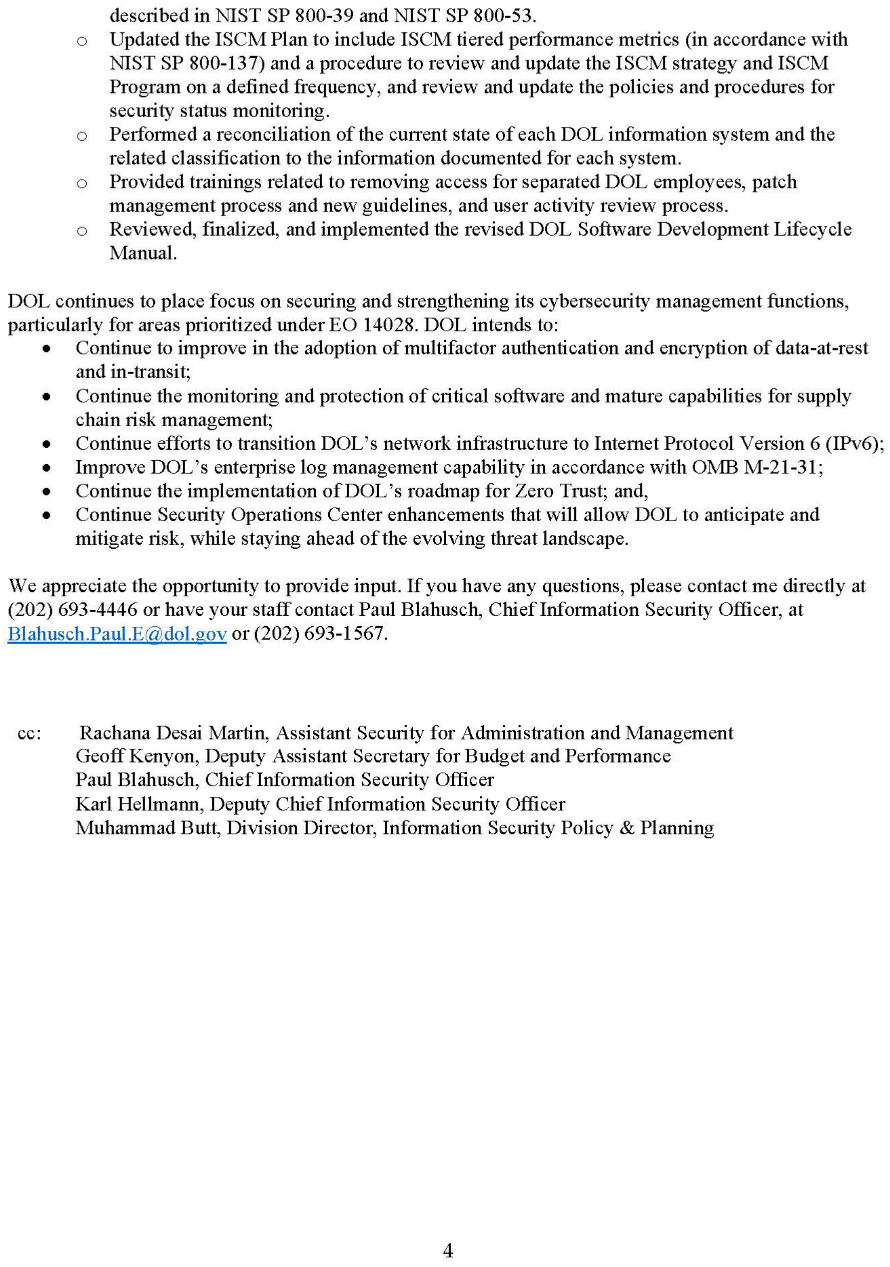
systems) was not included in the system's assessment plan, which ultimately had no bearing on system threats and vulnerabilities.

- **Risk:** Another finding in the report was that a single incident that was untimely reported to US-CERT (reported in 4 hours instead of the required 1 hour) increased risk to the confidentiality, availability, and integrity of DOL information systems and data. This was a single incident out of a sample of only 15 incidents tested by the auditors. DOL reported greater than 99.6% of 547 total incidents to US-CERT within the 1-hour reporting time during FY22. DOL Cyber responses to incident alerts has even been recognized by CISA as an example for other agencies to follow. This single incident was nonetheless rapidly resolved and ultimately presented no increased risk to the single system impacted, let alone to the Department. The report recommends enhanced incident response training to address this finding, which had in fact already been provided, and other measures already taken, prior to the auditors even identifying that issue. This is the very definition of being "Managed and Measurable". Although management presented these facts and examples of the maturity of the incident response program to the audit team, they chose not to consider this information or expand its sample and to focus exclusively on the results of the sample they selected instead of the universe of incidents.

We believe DOL has meaningful opportunities to improve the effectiveness of its cybersecurity program, and management remains committed to remediating cybersecurity risks, including through DOL's planned and on-track transition to NIST SP 800-53 Rev. 5. Unfortunately, this year's FISMA audit results, including the associated OIG FISMA metrics maturity level ratings, will not further this important goal.

Even though not reflected in the audit results, DOL worked diligently over the last year to implement changes to strengthen the maturity of its enterprise-wide cybersecurity program, and progress continues to be made to sustain cybersecurity maturity across all FISMA domains. Some of the significant changes made during FY 2022 include the following:

- Continued to enhance the cybersecurity program, including for areas prioritized under Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021).
- Continued to implement enterprise-wide solutions to enhance encryption, multifactor authentication, IT asset management, incident response and monitoring.
- Continued progress toward the deployment of Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation tools for vulnerability management.
- Continued implementation of new Data Loss Prevention mechanisms.
- Fully transitioned all FISMA systems into Ongoing Authorization.
- Conducted quarterly phishing exercises to promote phishing awareness.
- Continued to advance vulnerability management, which resulted in DOL being recognized by CISA for DOL's outstanding level of engagement on the Vulnerability Disclosure Policy Platform and DOL's commitment to its vulnerability awareness and management process.
- Continued to enhance incident response processes, resulting in DOL's cyber responses to incident alerts being recognized by CISA as a model for other agencies to follow.
- Successfully planned and carried out the FY 2022 DOL Cybersecurity Awareness Month.
- Closed 24 previously open cyber-related OIG findings from previous years.
- Made the following improvements based on OIG recommendations:
  - Developed and implemented a system that maintains and tracks DOL contractors who are required to have PIV cards.
  - Improved physical security processes by updating and improving emergency plan guidance, developed, and distributed active shooter training, and developed a process to automatically notify the Security Center when contractors are separated from DOL.
  - Updated the DOL Risk Management Strategy to appropriately address each activity and task



described in NIST SP 800-39 and NIST SP 800-53.

- Updated the ISCM Plan to include ISCM tiered performance metrics (in accordance with NIST SP 800-137) and a procedure to review and update the ISCM strategy and ISCM Program on a defined frequency, and review and update the policies and procedures for security status monitoring.
- Performed a reconciliation of the current state of each DOL information system and the related classification to the information documented for each system.
- Provided trainings related to removing access for separated DOL employees, patch management process and new guidelines, and user activity review process.
- Reviewed, finalized, and implemented the revised DOL Software Development Lifecycle Manual.

DOL continues to place focus on securing and strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. DOL intends to:

- Continue to improve in the adoption of multifactor authentication and encryption of data-at-rest and in-transit;
- Continue the monitoring and protection of critical software and mature capabilities for supply chain risk management;
- Continue efforts to transition DOL's network infrastructure to Internet Protocol Version 6 (IPv6);
- Improve DOL's enterprise log management capability in accordance with OMB M-21-31;
- Continue the implementation of DOL's roadmap for Zero Trust; and,
- Continue Security Operations Center enhancements that will allow DOL to anticipate and mitigate risk, while staying ahead of the evolving threat landscape.

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, at Blahusch.Paul.E@dol.gov or (202) 693-1567.

cc: Rachana Desai Martin, Assistant Security for Administration and Management
Geoff Kenyon, Deputy Assistant Secretary for Budget and Performance
Paul Blahusch, Chief Information Security Officer
Karl Hellmann, Deputy Chief Information Security Officer
Muhammad Butt, Division Director, Information Security Policy & Planning

APPENDIX D: FINDING REFERENCE

Finding #	Function	Domain	Issued Finding #
1	Identify	Risk Management	FISMA-22-01
2	Identify	Risk Management	FISMA-22-02
3	Protect	Configuration Management	FISMA-22-09
4	Protect	Identity and Access Management	FISMA-22-03
5	Protect	Data Protection and Privacy	FISMA-22-10 FISMA-22-11 FISMA-22-12
6	Detect	Information Security Continuous Monitoring	FISMA-22-06
7	Detect	Information Security Continuous Monitoring	FISMA-22-07
8	Respond	Incident Response	FISMA-22-04
9	Recover	Contingency Planning	FISMA-22-05

APPENDIX E: STATUS OF PRIOR-YEAR FINDINGS

As part of the FY 2022 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 2022 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 5 recommendations were closed and 15 recommendations remained open.

Table 6 describes the progress DOL has made in closing prior-year recommendations.

Table 6: DOL's Progress in Closing Prior-Year Recommendations

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
RM	FY 2019	Verify that annual assessments of third-party providers, including cloud service providers, are formally documented, reviewed, and signed by appropriate levels of management.	Open
RM	FY 2020	Provide training to responsible personnel over the third-party continuous monitoring review checklist.	Open
RM	FY 2020	We recommend the CIO complete, approve, and implement its Enterprise Architecture and related artifacts.	Open
RM	FY 2021	Enforce DOL requirements for authorizing connections and effective implementation of Interconnection Service Agreements.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
SCRM	FY 2021	Develop and implement a centralized process or mechanism for tracking monthly reviews of Cloud Service Providers.	Open
SCRM	FY 2021	Implement changes in oversight that enforce DOL requirements for the performance of the monthly continuous monitoring checklist for CSPs in accordance with the DOL CSH.	Open
CM	FY 2020	We recommend the CIO, 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 align DOL's goals and objectives.	Open
CM	FY 2020	Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process.	Open
IAM	FY 2019	Design and implement controls to perform and document a periodic review of audit logs that report privileged user activity.	Open
IAM	FY 2020	Provide training over the application user activity review process.	Open
IAM	FY 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.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
IAM	FY 2021	Implement a centralized process to monitor and enforce DOL requirements for completing proper background investigations based on position risk designations.	Closed
IAM	FY 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 policies.	Open
ISCM	FY 2019	Update the ISCM strategy guide with current ISCM performance metrics.	Closed
ISCM	FY 2021	Implement a process to enforce DOL's requirement that, when a change in AO occurs, the system authorization is reviewed, and a new authorization decision document is signed.	Closed
ISCM	FY 2021	Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of security control assessments.	Closed
IR	FY 2020	Provide additional resources to support operational activities during unforeseen circumstances.	Closed
CP	FY 2019	Develop and implement contingency planning performance metrics.	Open
CP	FY 2021	Enhance the OCIO monitoring and oversight of system owners to complete BIAs.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
CP	FY 2021	Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of contingency plan tests.	Open

APPENDIX F: GLOSSARY

ACRONYM	DEFINITION
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
ASA	Annual Security Assessment
BIA	Business Impact Analysis
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
CPP	Cybersecurity Policy Portfolio
CSAM	Cybersecurity Assessment Management
CSH	Computer Security Handbook
DHS	Department of Homeland Security
DIRA	Digital Identity Risk Assessment
DOL	United States Department of Labor
DPP	Data Protection and Privacy
EO	Executive Order
FAM	Financial Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IAM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer

ACRONYM	DEFINITION
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
Rev	Revision
RM	Risk Management
SCAP	Security Control Assessment Plan
SCRM	Supply Chain Risk Management
SP	Special Publication
ST	Security Training
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team

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

Online
http://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