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

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2021 FISMA DOL INFORMATION SECURITY REPORT: INFORMATION SECURITY CONTINUOUS MONITORING CONTROLS REMAIN DEFICIENT

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
Assistant Inspector General for Audit

DATE ISSUED: January 28, 2022
REPORT NUMBER: 23-22-001-07-725

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

BRIEFLY...

FY 2021 FISMA DOL INFORMATION SECURITY REPORT: INFORMATION SECURITY CONTINUOUS MONITORING CONTROLS REMAIN DEFICIENT

January 28, 2022

WHY OIG PERFORMED 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 audit on DOL's fiscal year (FY) 2021 information security program for the period October 1, 2020, through September 30, 2021. 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.

READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2022/23-22-001-07-725.pdf

WHAT THE AUDIT FOUND

KPMG reported 16 findings for DOL's information security program within 4 of 5 Cybersecurity Functions and 6 of 9 FISMA Metric Domains. Based on the CyberScope calculations and results, KPMG also determined DOL's information security program was not effective because a majority of the FY 2021 Inspector General (IG) FISMA Reporting Metrics were rated Consistently Implemented (Level 3).

A security program is only considered effective if the majority of the FY 2021 IG FISMA Reporting Metrics are rated at least Managed and Measurable (Level 4). Although DOL established and maintained its information security program and practices for its information systems for the five Cybersecurity Functions and nine FISMA Metric Domains, KMPG found weakness that demonstrated that the information security program had not achieved a Managed and Measurable (Level 4) in three of the five Cybersecurity Functions: Identify, Detect, and Recover.

The information security program's scores showed some improvements from FY 2020, which may indicate the continuing adoption and implementation of new tools to address the issues previously identified. However, based on the issues identified, we remain concerned about the remaining corrections needed in the Office of Chief Information Officer's (OCIO) oversight and accountability over the Department's information security control environment.

WHAT OIG RECOMMENDED

We made 18 recommendations for the specific issues identified in the systems identified in our scope of work, to strengthen DOL's information security program. Management generally concurred with the findings and recommendations identified and described in our report. OCIO stated it has addressed or will develop plans to address all recommendations.

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

INSPECTOR GENERAL'S REPORT

January 28, 2022

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) to conduct an independent audit of DOL's Fiscal Year (FY) 2021 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), and applicable American Institute of Certified Public Accountants (AICPA) standards.

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

PURPOSE

The objective of this audit was to determine if DOL implemented an effective information security program for the period October 1, 2020, to September 30, 2021. The determinations in this report were based, in part, on the testing of a selection of DOL's entity-wide and system-specific security controls across 20 of its information systems. Additional details regarding the scope of the independent audit are included in KPMG's report.

RESULTS

KPMG reported 16 findings for DOL's information security program in 4 of the 5 FISMA Cybersecurity Functions. These findings were based on the testing of 20 DOL systems and entity-wide controls, which notified the Chief Information Officer (CIO) of 45 control deficiencies and recommendations issued to respective system and entity-wide control owners.

These findings resulted in the U.S. Department of Homeland Security's (DHS) FISMA reporting system determining DOL's information security program was not effective for FY 2021. To be considered an effective information security program, DHS requires implementation of security controls to a level identified as Managed and Measurable (Level 4) for a majority of the Cybersecurity Functions. While results determined DOL's information security program had achieved a level of at least Consistently Implemented (Level 3) for all 5 Cybersecurity Functions, the weaknesses identified demonstrated that the program continue to not achieve the level of managed and measurable in three of the five Cybersecurity Functions: Identify, Detect and Recover.

Furthermore, while DOL received a Managed and Measurable (Level 4) rating within the Protect Function, additional progress is needed in two of its domains: Configuration Management and Identity and Access Management. DOL will need to focus on these two domains in order to maintain the overall level of Managed and Measurable (Level 4) for the Protect Function.

In reviewing the results from KPMG's testing, we are concerned the CIO's oversight over the Department's information technology is not ensuring progress on implementing Information Security Continuous Monitoring controls. In the Information Security Continuous Monitoring domain under the Detect Function, we continue to identify issues with the system authorization process, system security plans and security control assessments. The CIO needs to obtain authority and access to further implement robust monitoring capabilities, which continually assess the security state of the systems and hold the agency and system owners accountable for identified compliance gaps.

Additionally, in comparing the current year results to the FY 2020 FISMA assessment, we identified similar issues with access management, audit log review, and configuration management at the system level, which, due to the restructuring of DOL information technology, causes additional concern that the findings identified may also apply to other DOL systems.

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

Carolyn R. Hantz

INDEPENDENT AUDIT ON THE EFFECTIVENESS OF THE U.S. DEPARTMENT OF LABOR'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT – FISCAL YEAR 2021

January 25, 2022

kpmg.com

Contents

KPMG LETTER

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

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 2021

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 April 1, 2021, through September 30, 2021, and our results are through the period of October 1, 2020, through September 30, 2021.

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 that 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 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) 2021 Inspector General FISMA Reporting Metrics (FY 2021 IG FISMA Reporting Metrics). We responded to the FY 2021 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of the DOL Office of Inspector General (OIG). As part of our testing, we also followed up on the status of prior-year recommendations.

Consistent with applicable FISMA requirements, Office of Management and Budget (OMB) policy and guidance, and National Institute of Standards and Technology (NIST)

standards and guidelines, DOL established and maintained its information security program and practices for its information systems for the five Cybersecurity Functions and nine FISMA metric Domains. Based on the maturity levels calculated in CyberScope,[1] we determined DOL's information security program was not effective. A security program is considered effective if the majority of the FY 2021 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable. **Table 1** below depicts the maturity levels for the five Cybersecurity Functions.

Table 1: Maturity Levels for Cybersecurity Functions

Function	Maturity Level
Identify – Risk Management (RM) & Supply Chain Risk Management (SCRM)[2]	Consistently Implemented (Level 3)
Protect – Configuration Management (CM), Identity and Access Management (IAM), Data Protection and Privacy (DPP), and Security Training (ST)	Managed and Measurable (Level 4)
Detect – Information Security Continuous Monitoring (ISCM)	Consistently Implemented (Level 3)
Respond – Incident Response (IR)	Managed and Measurable (Level 4)
Recover – Contingency Planning (CP)	*Consistently Implemented (Level 3)*

Source: IG CyberScope entries

During FY 2021, we tested security controls at the entity level and for a selection of 20 systems. In addition, we conducted a targeted vulnerability assessment on selected devices for 12 of 20 selected DOL information systems. We identified and reported 16 findings in this report based on 45 notice of findings (NoFs) that we issued to DOL management. The control deficiencies were identified in 4 of the 5 FISMA Cybersecurity Functions and in 6 of the 9 FISMA Metric Domains. For example, we noted deficiencies in the performance of security control assessments, account management controls, and maintenance of system security plans (SSPs). We made 18 recommendations related to these control deficiencies that should strengthen DOL's information security program if effectively addressed by management. DOL should also implement a process to determine if these recommendations apply to other information systems maintained in its FISMA inventory. Furthermore, the OCIO should 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.

We also evaluated the implementation of recommendations from prior FISMA reports. Out of 43 previously open recommendations related to FY 2018 and

[1] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline 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. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

[2] According to the FY 2021 IG FISMA Reporting Metrics, we assessed the maturity levels of the SCRM metrics, but they are not considered in the overall maturity results used in determining the effectiveness of the Identify Function and the overall information security program.

2019 FISMA evaluations and FY2020 FISMA performance audit, we determined DOL has successfully closed 11 recommendations.

KPMG 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, Department of Homeland Security (DHS), and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

January 25, 2022

BACKGROUND, OBJECTIVE, SCOPE AND METHODOLOGY

BACKGROUND

KPMG performed the FY 2021 independent FISMA evaluation under contract with DOL as a performance audit in accordance with GAGAS. The DOL 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 employers and 125 million workers.

PROGRAM OVERVIEW

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 best in class 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 is 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.

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

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 purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and provide 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 OMB with respect to agency information security policies and practices, and (2) set forth the authority for the Secretary of the DHS to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials 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

For FY 2021, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) continued to develop the FY 2021 IG FISMA Reporting Metrics, Version 1.1, dated May 12, 2021, around five Cybersecurity Functions[3] outlined in the NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[4] (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover. In addition, the FY 2021 IG FISMA Reporting Metrics use the CIGIE maturity models for the nine FISMA Metric Domains: RM, SCRM, CM, IAM, DPP, ST, ISCM, IR, and CP. **Table 2** outlines the alignment of the Cybersecurity Framework Functions to the FISMA Metric Domains.

[3] In its *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, 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.

[4] The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 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 Executive Order 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.

Table 2: Alignment of the NIST Framework for Improving Critical Infrastructure Cybersecurity Functions to the FISMA Metric Domains within the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Functions	FISMA Metric Domains
Identify	RM SCRM
Protect	CM IAM DPP ST
Detect	ISCM
Respond	IR
Recover	CP

Source: FY 2021 Inspector General FISMA Reporting Metrics v1.1

Changes for FY 2021

The FY 2021 IG FISMA Reporting Metrics included a new Domain, SCRM, within the Identify Function. This new Domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that external providers' products, system components, systems, and services are consistent with the organization's cybersecurity. The new Domain references SCRM criteria in NIST Special Publication (SP) 800-53, Revision (Rev) 5, *Security and Privacy Controls for Information Systems and Organizations*. To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5, in accordance with OMB Circular A-130, these new metrics are not considered for the Identify framework Function rating in FY 2021. The RM Domain was reorganized to focus on the cyber RM process and how an agency integrates with its enterprise RM process. Furthermore, the IG metric questions have been streamlined to reduce redundancies.

OMB provided guidance for agencies to improve vulnerability identification, management, and remediation by issuing OMB Memorandum M-20-32, *Improving Vulnerability Identification, Management, and Remediation*. DHS issued Binding Operational Directive 20-01, *Develop and Publish a Vulnerability Disclosure Policy,* which provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures. This resulted in changes to the CM Domain area.

IG FISMA Scoring

With the exception of SCRM, the ratings in the eight Domains (RM, CM, IAM, DPP, ST, ISCM, IR, and CP) were determined by a simple majority, where the most frequent level (mode) [5] for the questions was the Domain rating. When responses are entered, the calculations were performed by CyberScope and determined the rating for each Domain and Function.

The maturity model has five levels: Level 1: Ad-hoc, Level 2: Defined, Level 3: Consistently Implemented, Level 4: Managed and Measurable, and Level 5: Optimized. **Table 3** details the five maturity levels to assess the agency's information security program for each Cybersecurity Framework Function. A security program is considered effective if a simple majority of the FY 2021 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable.

Table 3: Inspector General Assessed Maturity Levels

Maturity Level	Description
Level: 1 Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level: 2 Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	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.
Level 5: Optimized	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 FISMA Reporting Metrics v1.1

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.

[5] The FY 2021 IG FISMA Reporting Metrics introduced a new pilot concept of weighting ten priority FISMA metrics for assessment and scoring. As part of the proposed weighted average approach to scoring, these priority metrics would be weighted twice as much in the maturity calculation. The simple majority scoring will still be used in calculating the overall scoring for FY 2021; however, the weighted average pilot will help the DOL evaluate the impact of the scoring change in the event it is implemented in the future.

OBJECTIVE, SCOPE AND METHODOLOGY

OBJECTIVE

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 Function areas outlined in the FY 2021 IG FISMA Reporting Metrics. We responded to the FY 2021 IG FISMA Reporting Metrics and assessed the maturity levels on behalf of DOL OIG. As part of our testing, we also followed-up on the status of prior-year findings.

SCOPE

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2021 IG FISMA Reporting Metrics; applicable NIST standards and guidelines, presidential directives, and OMB memorandums referenced in the reporting metrics; and the DOL Computer Security Handbook (CSH).[6] 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 (15 federal and 5 contractor information systems) from a total population of 80 information systems as of March 9, 2021. 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

[6] The CSH provides IT security policies, procedures, standards, and guidance aligned to NIST guidance and DOL's risk appetite and business prerogatives to those involved in the planning, development and operation of information systems.

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 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.

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.

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

- Inquiry of information system owners, Information System Security Officers (ISSOs), 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; and
- Execution of a targeted vulnerability assessment on selected devices for nine in-scope DOL information systems.

We performed our fieldwork from April 1, 2021, through September 30, 2021. Due to the COVID-19 pandemic, all testing was performed remotely through virtual meetings, walkthroughs, and observations with representatives of DOL. During our performance audit, we met with DOL management and the OIG remotely to discuss our findings.

CRITERIA

We focused our FISMA performance audit approach on federal information security guidance developed by NIST and OMB. NIST SP provides guidelines that are essential to the development and implementation of agencies' security programs. We also utilized DOL's CSH, which outline DOL's requirements for information security. For each deficiency detailed in the “Audit Findings and Recommendations” section, we included the relevant DOL and NIST criteria.

OVERALL RESULTS

RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, DOL established and maintained its information security program and practices for its information systems for the five Cybersecurity Functions and nine FISMA Metric Domains. Based on the maturity levels calculated in CyberScope, we determined DOL's information security program was not effective. A security program is considered effective if the majority of the FY 2021 IG FISMA Reporting Metrics are at least Level 4: Managed and Measurable. **Table 4** below depicts the maturity levels for the five Cybersecurity Functions.

Table 4: Maturity Levels for Cybersecurity Functions

Function	Maturity Level
Identify – RM & SCRM[7]	Consistently Implemented (Level 3)
Protect – CM, IAM, DPP, and ST	Managed and Measurable (Level 4)
Detect – ISCM	Consistently Implemented (Level 3)
Respond – IR	Managed and Measurable (Level 4)
Recover – CP	Consistently Implemented (Level 3)

Source: IG CyberScope entries

During FY 2021, we tested security controls at the entity level and for a selection of 20 systems. In addition, we conducted a targeted vulnerability assessment on selected devices for 12 of 20 selected DOL information systems. We identified and reported 16 findings in this report based on 45 notice of findings (NoFs) that we issued to the DOL management. The findings were identified in 4 of the 5 FISMA cybersecurity functions and in 6 of the 9 FISMA Metric Domains. We also evaluated the implementation of recommendations from prior FISMA reports. Out of 43 previously open recommendations related to FY 2018 and 2019 FISMA evaluations and FY2020 FISMA performance audit, we determined DOL has successfully closed 11 recommendations.

IDENTIFY

The objective of the *Identify* Function in the Cybersecurity Risk 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

[7] *Supra* note 2.

prioritize RM decisions. We assessed DOL's Identify Function at the Consistently Implemented maturity level. As described in detail below, we found that, while DOL developed and propagated risk management policies and procedures, our testing found issues in its implementation of RM and SCRM security controls. Additionally, DOL has not defined SCRM strategies, policies, and procedures to manage supply chain risks.

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 that has been developed to address the various risks 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. We determined DOL has implemented policies and procedures to maintain a complete and accurate inventory of its major information systems, hardware devices, and software. DOL performs 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.

DOL updated its RM strategy to better align it with NIST SP 800-39, *Managing Information Security Risk*. The updated RM strategy provided more specific guidance for each RM tier (organization, mission/business processes, and information systems) and steps within the RM process (framing risk, assessing risk, responding to risk, and monitoring risk). Lastly, DOL created a more rigorous strategy to monitor risks.

DOL has developed and implemented processes for authorizing information systems, performing risk assessments, developing and implementing secure architecture, and tracking and monitoring Plans of Action and Milestones (POA&Ms). DOL utilizes the Continuous Diagnostics and Mitigation (CDM) program to provide enterprise IT security reports and dashboards. Further, the Cybersecurity Assessment Management (CSAM) tool is the primary source for obtaining risk data. DOL stakeholders use these processes to identify, manage, and track cybersecurity risks that OCIO incorporates into DOL's risk register.

However, based on the results of our test procedures, we found instances in which management would informally accept risk, rather than identify, assess, and respond to risk following DOL's formal RM process. Additionally, DOL did not ensure that its SSPs accurately documented the security posture of its systems. Control implementation statements did not accurately reflect the current system environment, and security controls required per NIST SP 800-53, Rev. 4, were not included in the SSPs.

For additional information regarding the RM issue identified, see Finding 1.

SUPPLY CHAIN RISK MANAGEMENT

SCRM requires agencies 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 domain as Ad Hoc. We determined that DOL has not defined SCRM policies, procedures, and strategies. For most of the performance audit period, DOL was developing its SCRM strategy, policies, and procedures.

The SCRM FISMA Metric Domain was new to the FY 2021 FISMA IG Reporting Metrics; however, supply chain risks are not new to the federal sector as demonstrated by the Federal Acquisition Supply Chain Security Act of 2018. According to the FY 2021 IG FISMA Reporting Metrics, the SCRM overall maturity results were not used in determining the effectiveness of DOL's overall information security program.

For additional information regarding the SCRM issue identified, see Finding 2.

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. This Function is carried out by proper CM, IAM, DPP, and ST controls and processes. We assessed DOL's *Protect* Function at the Managed and Measurable maturity. While we found that DOL developed and propagated policies, procedures, and guidance for CM, IAM, DPP and ST, our testing found issues in its implementation and

operating effectiveness of security controls in the CM and IAM FISMA Metric Domains.

CONFIGURATION MANAGEMENT

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

Based on the results of our performance audit procedures, we assessed DOL's CM FISMA Metric Domain as Consistently Implemented. While we found that DOL developed and propagated CM policies and procedures, our testing found issues in the implementation and operating effectiveness of CM controls related to unimplemented prior year recommendations and control deficiencies identified in this year's performance audit. We also found that DOL had not implemented meaningful qualitative and quantitative metrics related to the FISMA domain.

We determined DOL improved its ability to generate data relating to its performance of CM processes through the use of more sophisticated CM technology; however, the performance metrics were not formalized to determine the effectiveness of its CM plan. Additionally, management did not consistently document CM controls for three information systems tested and did not consistently perform security impact analyzes prior to the implementation of changes.

We determined DOL consistently records, implements, and maintains baseline configurations of its information systems and an inventory of related components in accordance with its policies and procedures. DOL uses tools to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for its information system components connected to its network. However, DOL has not established a process to manage deviations to its baseline configurations of its information systems.

DOL centrally manages its flaw remediation process and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its flaw remediation processes. DOL utilizes a vulnerability disclosure policy as part of its vulnerability management program for internet-accessible federal systems. However, we identified instances where DOL does not remediate software vulnerabilities within the timeframes defined in DOL's CSH.

We noted that DOL has not implemented Trusted Internet Connections 3.0 in accordance with OMB M-19-26.

For additional information regarding the CM issues found, see Findings 3 through 6.

IDENTITY AND ACCESS MANAGEMENT

The IAM Domain includes the requirement that an agency implement a set of capabilities to ensure that users authenticate to IT resources and have access to only those 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 (ICAM).

Based on the results of our performance audit procedures, we assessed DOL's IAM FISMA Metric Domain as Consistently Implemented. While we noted that DOL developed and propagated IAM policies and procedures, our testing found issues in its implementation and operating effectiveness of IAM security controls related to unimplemented prior year recommendations and control deficiencies identified in this year's performance audit.

We determined that DOL has developed an ICAM strategy that has defined specific milestones to track its progress. DOL utilizes its ICAM architecture when developing new applications and continues to integrate its legacy applications into its modern ICAM architecture. As in past years, DOL continues to make progress in implementing single sign-on (SSO) for its applications, including the use of Login.gov for external users.

DOL continues to implement new capabilities to automate the account management of information system privileged and non-privileged accounts. DOL has defined a process for providing Personal Identity Verification (PIV) exemptions to non-privileged users but does not consistently follow this process. Furthermore, DOL has not met federal targets for the implementation of the identity proofing and authentication processes (IAL/AAL) level 3 for non-privileged users. We identified instances in which DOL did not consistently complete user authorization forms appropriately or maintain Rules of Behavior (ROB) forms for privileged users.

DOL implemented processes to drive higher compliance in manual access controls, such as the biannual privileged user account review and user activity audit log reviews. Although we identified ineffective user account review controls,

the overall number of such deficient controls decreased from the prior years. DOL still inconsistently performed and documented privileged user activity audit log reviews.

DOL ensures that Federal Information Processing Standard Publication (FIPS) 140-2 validated cryptographic modules are implemented for its remote access connection methods. However, DOL did not perform host-based scanning prior to allowing remote access to workstations.

For additional information regarding the IAM issues found, see Findings 7 through 9.

DATA PROTECTION AND PRIVACY

DPP refers to a collection of activities focused on the security objective of confidentiality, preservation of authorized restrictions on information access, and 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 their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *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 proper implementation of the NIST Risk Management Framework (RMF). Although the head of each federal agency remains ultimately responsible for ensuring that privacy interests are protected and for managing PII responsibly within their agency, Executive Order 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 performance audit procedures, we assessed DOL's DPP FISMA Metric Domain as Managed and Measurable. As in previous years, we identified that DOL did not sufficiently encrypt data-at-rest; however, we found that DOL consistently implemented its DPP policies and procedures and utilized quantitative and qualitative measures to evaluate the effectiveness of its DPP program.

We determined DOL performs data exfiltration tests and cyber exercises to analyze the performance of its enhanced network defenses and the effectiveness of its Data Breach Response Plan. Further, DOL measures the effectiveness of its privacy awareness training program through feedback received from users

that complete the privacy awareness training and phishing exercises. Also, DOL did not consistently encrypt PII data-at-rest at the server level.

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 performance audit procedures, we assessed DOL's ST domain as Managed and Measurable. We found that DOL developed and propagated security training policies and procedures, and our testing did not find any reportable issues. DOL monitors performance measures on the effectiveness of its security awareness and training strategies, plans, and programs through capturing course evaluation statistics, performing analysis over phishing exercise results, and updating training based on feedback received from users and evolving threats and risks.

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 performance audit procedures, we assessed DOL's *Detect Function* and the aligned ISCM FISMA Metric Domain as Consistently Implemented. We found that DOL developed and propagated ISCM policies and procedures, but our testing found issues in the operating effectiveness of ISCM controls, most notably as it related to system authorization and periodic security control assessments.

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.

We determined DOL management has a defined ISCM strategy and has implemented some qualitative and quantitative measures to support visibility into its assets. DOL was still transitioning information systems to ongoing

authorization. DOL was not maintaining system authorizations or performing system control assessments in compliance with the CSH.

For additional information regarding the information security continuous monitoring issues found see Findings 10 through 13.

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 performance audit procedures, we assessed DOL's *Respond* Function and the aligned IR FISMA Metric Domain as Managed and Measurable. We did not identify any testing exceptions or deficiencies with DOL's IR program and associated security controls. DOL implemented IR policies, procedures, plans, strategies, and technologies. DOL monitors and analyzes the effectiveness of its incident response policies, procedures, plans, strategies, and technologies through weekly reports that capture IR activities. DOL utilizes multiple advanced tools to support the IR processes. These tools feed into DOL's Security Information and Event Management (SIEM) tool to give a centralized view of the incidents. Further, DOL utilizes profiling techniques to maintain a comprehensive baseline of network operations and expected data flows for users and systems.

DOL utilizes its threat vector taxonomy to classify incidents and capture metrics over the incidents reported in accordance with United States Computer Emergency Readiness Team (US-CERT) guidelines. Additionally, DOL captures the impact of incidents and uses the information to mitigate related vulnerabilities on other systems.

RECOVER – CONTINGENCY PLANNING

The objective of the *Recover* Function in the Cybersecurity Framework is to ensure that 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 performance audit procedures, we assessed DOL's *Respond* Function and the aligned CP FISMA Metric Domain as Consistently Implemented. While we found that DOL developed and propagated CP policies and procedures, our testing found issues in its operating effectiveness of its CP security controls. We, also, found that DOL lacked meaningful qualitative and quantitative metrics related to CP.

We determined DOL implemented its policies, procedures, processes, strategies, and technologies for information system backup and tests its information system CP in accordance with the DOL CSH. However, DOL needs to develop qualitative and quantitative performance metrics and monitor them to determine the effectiveness of its *Recover* Function. DOL did not consistently enforce the requirement that personnel with CP responsibilities undergo training on an annual basis and did not producing metrics on the effectiveness of recovery activities.

For additional information regarding the contingency planning issues found see Findings 14 through 16.

AUDIT FINDINGS AND RECOMMENDATIONS

IDENTIFY – RISK MANAGEMENT

FINDING 1: INTERCONNECTION SECURITY AGREEMENTS WERE NOT AUTHORIZED

For one system tested, one of two Interconnection Security Agreements (ISAs) selected did not include appropriate signatures for authorization.

The DOL CSH states agencies are required to authorize connections from their information systems to other information systems using ISAs. The Authorizing Official (AO) uses ISAs to formally authorize connections between DOL's information systems and other information systems outside of DOL's system authorization boundaries.

This occurred due to inadequate management oversight by the OCIO personnel responsible for ensuring security documentation was completed in accordance with the CSH.

Failure to appropriately authorize the ISA could lead to a misunderstanding of the technical framework for agreed upon security controls and defined responsibilities for data shared between two systems. This, in turn, could result in the failure of one or both system owners/interfacing parties to perform controls that help ensure the confidentiality, integrity, and availability of DOL data and other sensitive information.

We recommend the CIO:

1. Enforce DOL requirements for authorizing connections and effective implementation of Interconnection Service Agreements.

IDENTIFY – SUPPLY CHAIN RISK MANAGEMENT

FINDING 2: CLOUD SERVICE PROVIDER CHECKLISTS WERE NOT COMPLETED

The monthly continuous monitoring checklist for one Cloud Service Provider (CSP) associated with one of the systems tested was not completed and signed for one of two months selected.

For another system tested, the continuous monitoring checklists for one CSP were completed on a quarterly basis instead of the required monthly frequency per DOL CSH; therefore, evidence of the monthly review was unavailable.

The DOL CSH states that at a minimum, the continuous monitoring review and corresponding checklist is required to be completed on a monthly frequency for third-party contractors, including CSPs.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring security reviews of CSPs were performed as required the CSH.

Failure to conduct the third-party continuous monitoring checklist appropriately could lead to an increase in undetected security risks, which could result in a compromise of the integrity, confidentiality, and security of the agency's information systems.

We recommend the CIO:

2. 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.

3. Develop and implement a centralized process or mechanism for tracking monthly reviews of CSPs.

PROTECT – CONFIGURATION MANAGEMENT

FINDING 3: BASELINE CONFIGURATIONS WERE NOT MAINTAINED

For one system tested, DOL did not perform the annual configuration audit to assess the current physical and functional configurations that support the system to identify any deviations from the system-approved baseline configuration. Due to competing priorities during the reorganization of the IT Asset and Configuration Management Branch, DOL management postponed the annual configuration audit. Management did not obtain a formal risk waiver for postponing the operation of this control.

For one system tested, management did not enforce the configuration baselines for system's servers. Also, evidence of management's annual information system

component inventory review for the system was not available due to COVID-19, as resources were focused on transitioning the agency to a remote work environment.

For one system tested, the hardware inventory listing did not include documentation of the manufacturer, model number, and serial number, as required by the DOL CSH. Management informed us that this condition occurred due to lack of management oversight.

DOL's Change Management Plan states effective CM requires regular evaluation of the configuration through the execution of the auditing function, where the physical and functional configurations are compared to the documented configuration. Configuration audits are performed annually and are submitted to Configuration Change Management (CCM) for review. Also, the CSH states that the baseline configuration of the information system must be reviewed and updated at least annually or when a major change occurs.

The DOL CSH states agencies must establish and implement configuration settings for IT products employed within the information system using agency-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements.

Further, the DOL CSH states agencies must review and update the information system component inventory when a system change occurs or at least on an annual basis. The requirements for developing and documenting an information system component inventory should:

- Accurately reflect the current information system.
- Include all components within the authorization boundary of the information system.
- Determine the appropriate level of granularity deemed necessary for tracking and reporting.
- Include system-specific information deemed necessary for effective accountability of information system components including, but is not limited to:
  - Manufacturer,
  - Model number,
  - Serial number,
  - Software (to include license information as required), and
  - System/component owner.

These issues occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring that configuration baselines and security documentation are complete and accurate.

Failure to record, implement, and maintain baseline configurations of its information systems could result in DOL's inability to detect ineffective change and configuration management policies, procedures, and control activities. In addition, without the monitoring and controlling of changes to the configuration settings, loss of the confidentiality, integrity, and availability of DOL's information systems could occur.

Without an accurate and detailed hardware inventory list, the necessary information for effective accountability of information system components may not be retained.

We recommend the CIO:

4. Enforce DOL requirements for implementing, auditing, testing and documenting exceptions to baseline configurations.

5. Ensure DOL maintains a complete and accurate inventory of its hardware and software assets.

FINDING 4: ANNUAL REVIEW OF SERVICES, FUNCTIONS, PORTS, AND PROTOCOLS WAS NOT PERFORMED

For one system tested, controls were not designed, and procedures were not documented to conduct an annual review of unsecure functions, ports, protocols, and services for the system's environment. Management utilized Nessus scans to meet the DOL CSH requirement, in place of performing a formal review; however, the review of the scans was not documented. Further, NIST SP 800-53 Rev. 4 requires organizations to review functions and services provided by information systems or individual components of information systems to determine which functions and services are candidates for elimination. Nessus scans do not provide the information necessary to support such decision making.

The DOL CSH states that agencies must review the information system at least on an annual basis to identify unnecessary and/or non-secure functions, ports, protocols, and services. Also, control CM-7 Least Functionality in NIST SP 800-53 Rev. 4 provides additional guidance to perform the review.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring compliance with this requirement.

Failure to perform the review of information systems increases the risk of unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

We recommend the CIO:

6. Enhance the management oversight by OCIO to enforce DOL requirements for the performance of annual reviews of unsecure functions, ports, protocols, and services.

FINDING 5: SECURITY IMPACT ANALYSIS TO CHANGES WAS NOT PERFORMED

For four systems tested, supporting documentation evidencing that Security Impact Analysis (SIAs) were performed prior to the implementation of information system changes was not available

The DOL CSH states that, prior to system change implementation, and as part of the change authorization process, DOL management should analyze changes to the information system for potential security impacts.

This occurred due to lack of management oversight by OCIO personnel responsible for ensuring that security documentation was retained appropriately.

Without analyzing system changes for potential security impacts, a change may be implemented that has security ramifications affecting the effectiveness of other controls or create new security risks that are unmitigated.

We recommend the CIO:

7. Execute the OCIO and AO oversight process to ensure compliance with DOL requirements for the performance of SIAs prior to the implementation of system changes.

FINDING 6: VULNERABILITY MANAGEMENT PROCESS WAS NOT IMPLEMENTED

For three general support systems tested, the vulnerability management process was not properly implemented. Specifically, we noted the following:

- For one system tested, we sampled 15 devices and identified 17 high vulnerabilities and 272 medium vulnerabilities as not mitigated or properly documented in a POA&M, within the DOL CSH required timelines.

- For another system tested, we sampled 33 devices and identified 1 critical vulnerability and 14 medium vulnerabilities as not mitigated or properly documented in a POA&M, within the DOL CSH required timelines.

- For another system tested, we sampled 22 devices and identified 1 critical vulnerability and 14 medium vulnerabilities as not mitigated or properly documented in a POA&M, within the DOL CSH required timelines.

The CSH requires mitigation recommendations based on the risk assessment and the control assessment results to be captured in a POA&M and maintained and tracked as part of the Department's POA&M management process.

The CSH also establishes the minimum requirements for installing updates on information systems including:

a. Updates identified as critical importance (including all out of cycle updates) must be installed within 10 business days of release.
b. Updates identified as high importance must be installed within 15 business days of release.
c. Updates identified as moderate importance must be installed within 20 business days of release.
d. Updates identified as low importance must be installed within 30 business days of release.

For three general support systems tested, vulnerabilities were not remediated or documented within the DOL established timeframes due lack of sufficient resources to appropriately handle both operational and security requirements.

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

We recommend the CIO:

8. Implement a centralized process to monitor vulnerabilities for information systems to ensure that each vulnerability is remediated within the CSH defined timeframe.

PROTECT – IDENTITY AND ACCESS MANAGEMENT

FINDING 7: APPROPRIATE BACKGROUND INVESTIGATION WAS NOT PERFORMED

For one agency, management did not complete a background investigation for one of three individuals selected for testing commensurate with their personnel risk designation. The agency informed us the lapse occurred because the agency does not require a second level review of the background investigation report.

In accordance with Office of Personnel Management policy, DOL establishes position risk designation to all organizational positions. The position risk designation establishes the sensitivity level of the position, and subsequently, the level of background investigation that must be conducted to individuals to fill the position. The DOL CSH states that management shall screen individuals requiring access to Department systems before authorizing access according to the DOL policy outlined in the Personnel Suitability and Security Handbook for the individuals' position risk designations of the assigned positions.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring suitability determinations are commensurate with the position are complete and accurate.

Failure to perform adequate background investigations for employees and contractors could lead to the use of DOL systems by inappropriately vetted individuals, potentially exposing sensitive data.

We recommend the CIO:

9. Implement a centralized process for OCIO to ensure a proper background investigation has been completed prior to activating any information system accounts associated with the individual.

FINDING 8: USER ACCOUNT MANAGEMENT CONTROLS WERE NOT FOLLOWED

For one system tested, the signed ROB forms for 2 of 2 privileged users were unavailable as the system that stored the forms was decommissioned. For another system, the signed ROB forms for 15 of 15 privileged users were also

unavailable as management stated they were unaware of the requirement to retain ROB acknowledgements throughout the duration of the users' access.

For one system tested, DOL did not document access authorizations for two of the five selected users based on a valid need-to-know justification. Management stated that these deficiencies occurred due to a lack of management oversight.

For one system tested, management did not implement a formal process to authorize new administrators. Additionally, the review of system administrators was performed on an annual basis, instead of the required biannual frequency. Further, management did not retain supporting documentation evidencing the initial approval and periodic review of administrators. Management stated that this finding was caused by the prioritization of resources on transitioning the agency to a remote work environment during the COVID-19 pandemic.

The DOL CSH states the system owner is responsible for ensuring that a record is maintained showing that users have acknowledged receipt of the ROB. Due to the higher level of risk and responsibility associated with privileged information system users, DOL requires privileged users to acknowledge the privileged ROB. This information should be maintained throughout the entire duration of the users' system access.

The DOL CSH states the system owner (or Agency representative designated by the AO) shall authorize access based on a valid need-to-know/need-to-share justification that is determined by the user's assigned official duties. Further, all access request forms must be maintained for one year after account deletion. Also, the DOL CSH states information system accounts should also be reviewed every six months to verify and validate (recertify) that all active privileged and non-privileged user accounts are still required based on user need and rights.

Acquiring system access before completing ROBs increase the risk that users do not understand security requirements set forth in the ROB. This could lead to an individual inadvertently exposing a system to compromise from internal and external threats. Further, failure to maintain the acknowledgement of the ROB may make it difficult to hold users accountable in instances of inappropriate system usage.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring the appropriate access authorizations are gathered prior to the provisioning access and that ROB acknowledgements are retained in accordance with the CSH.

Failure to appropriately authorize new information system users could result in the assignment of excessive access and/or access privileges that result in

segregation of duties conflicts. Also, failure to complete formal biannual administrator reviews could lead to an increased risk of unauthorized access to and modification of production data and computing resources.

We recommend the CIO:

10. Implement a control to retain rules of behavior acknowledgements, access authorizations, other required documentation for authorized system access, and periodic user access reviews. OCIO should monitor this control to ensure each FISMA-reportable system is compliant with the DOL CSH account management policies.

FINDING 9: AUDIT LOGS WERE NOT REVIEWED

For two systems tested, audit logging capabilities were not enabled; therefore, audit logs were not generated and retained.

For one system tested, the monthly audit log review was not performed on a timely basis for one of two months selected due to lack of management oversight.

For one system tested, management did not retain evidence that audit logs were reviewed for each of the two months sampled for testing. Management informed us that it only documented its review when unusual or suspicious activity was identified and that, for the months tested, no such activity was identified.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring system auditing was appropriately configured and audit logs were reviewed and maintained.

The DOL CSH states DOL information systems shall produce audit records that contain sufficient information to establish what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any user or subject associated with the event. Additionally, 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.

Without logging and reviewing the activity of DOL user accounts, management may not be able to detect and timely address unauthorized access of and/or modification to DOL information system computing resources and production data.

We recommend the CIO:

11. Strengthen the OCIO controls to monitor system owners to ensure they implement appropriate audit logging controls in accordance with the CSH.

DETECT – INFORMATION SECURITY CONTINUOUS MONITORING

FINDING 10: NEW AUTHORIZING OFFICIAL DID NOT REVIEW SYSTEM AUTHORIZATION TO OPERATE PACKAGES

As part of the Enterprise Shared Services Initiative within DOL, IT operations has been consolidated under OCIO. As IT operations were transitioned to OCIO, the designated AO for those systems was changed to the CIO. As part of this initiative, management transitioned 46 information systems to OCIO. For 4 of the 20 systems tested, we noted that the AO was changed to the CIO. After being designated as the AO, the CIO did not follow the DOL CSH and sign new authorization decision documents for each of the 4 aforementioned systems.

A formal memorandum designated the CIO as the AO for each system transitioned to OCIO as part of the Enterprise Shared Services Initiative. The OCIO informed us that the CIO participated in monthly briefings over the IT security posture of the systems. The OCIO further informed us, contrary to the DOL CSH, it was understood by DOL management that briefings regarding the transitioned systems and the signed AO Designation Memo constituted an acceptance of the risk associated with the systems.

This occurred as the CIO did not follow DOL policies and procedures for authorizing systems. Although the CIO may have understood the risk to DOL associated with the operation of these systems, the signed authorization decision document serves as the official, formal transfer of the AO's responsibility for the systems. Without the signed document, the transitioned systems were effectively unauthorized and did not have a single, accountable AO.

The DOL CSH states if there is a change in AOs for a system, the new AO reviews the current authorization decision document, authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new AO is willing to accept the currently documented risk, the CSH states that the AO signs a new authorization decision document, thus formally transferring responsibility for the system and accepting the risk to organizational operations and assets, individuals, and other organizations, and the Nation.

Failure of the newly designated AO to explicitly approve authorization decision documents results in a lack of formally established and documented responsibility and accountability for the information systems. This may lead to the AO not understanding the inherent and residual risks and the internal and external threats and vulnerabilities to the system. This increases the risk that controls and mitigations may not be prioritized, evaluated, and implemented appropriately.

We recommend the CIO:

12. Implement a process to enforce DOL's requirement for, when a change in AO occurs, that the system authorization is reviewed, and a new authorization decision document is signed.

FINDING 11: SYSTEM SECURITY PLANS WERE NOT MAINTAINED

For seven systems tested, the controls to develop and review SSPs were not operating effectively. For each of these seven selected systems, we identified that security controls were inaccurately documented in their respective SSPs. In some cases, changes had occurred in the system environments, and the SSPs were not updated accordingly. In others, the controls documented in the SSPs did not sufficiently capture the requirements of NIST SP 800-53 controls. For example, one system SSP's description of control CM-8, Information System Component Inventory, did not describe the means by which information system components were documented to effectively support tracking and reporting. Another system SSP's description of control CM-3, Configuration Change Control, did not include a defined retention period for configuration-controlled changes. Additionally, guidance per NIST SP 800-18 was not followed to review and update the SSPs, as needed.

For four systems tested, the SSP was not adequately reviewed and updated annually. For one system, the scoping guidance was not applied accurately; therefore, the controls were not accurately documented in the SSP as they did not reflect the system's current control environment. For two systems tested, the SSP was not updated to reflect the current system status. For example, one system SSP inaccurately described control Identification and Authentication (IA)-5 Authenticator Management, as inherited.

This occurred due to inadequate review and oversight by the OCIO personnel responsible for ensuring security documentation is complete and accurate, human error, and lack of adequate resources.

The DOL CSH states that agencies must develop and implement SSPs for its information systems that provide an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Additionally, NIST SP 800-18, Rev 1, provides the guidance for developing SSPs and states that it is important to periodically assess the plan; review any change in system status, functionality, or design; and ensure that the plan continues to reflect the correct information about the system.

Without accurate implementation statements within the SSP, there is an increased risk that controls are not implemented correctly, or the AO approves a system without fully understanding the controls in place to mitigate the risks to the system.

We recommend the CIO:

13. 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 12: SYSTEMS DID NOT IMPLEMENT CONTINUOUS MONITORING STRATEGY

For one system tested that follows the ongoing authorization process, DOL did not develop a system-level continuous monitoring strategy. The OCIO stated that it believed that a system-level continuous monitoring strategy was not necessary as the OCIO had a defined enterprise-wide ISCM strategy and plan. NIST SP 800-37, Rev. 2, states, “consistent with the organizational monitoring strategy, [the system-level ISCM strategy] defines how changes to the system and the environment of operation are to be monitored; how risk assessments are to be conducted; and the security and privacy posture reporting requirements including the recipients of the reports.”

For one system tested, the system’s ISCM strategy did not include all requirements in accordance with NIST SP 800-53, Rev. 4, control CA-07 – Continuous Monitoring. Specifically, the ISCM strategy did not include the analysis of security-related information generated by assessments and monitoring, response actions to address results of the analysis of security-related information, and the reporting of the security status of organization and the information system to appropriate personnel. Management stated that it did not prioritize updating the ISCM strategy for this system.

NIST SP 800-37, Rev. 2, states systems are required to develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organization continuous monitoring strategy.

NIST SP 800-53, Rev. 4, states:

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [Assignment: organization-defined metrics] to be monitored;
b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

This occurred due to inadequate oversight by OCIO personnel responsible for developing and implementing DOL's ISCM strategy.

Failure to develop and follow a system-level ISCM strategy presents a risk that system controls may not be appropriately monitored by the AO. This failure could lead to an increased risk that security vulnerabilities or weaknesses exist and are not identified and addressed in an appropriate manner.

We recommend the CIO:

14. Enhance the OCIO oversight of the DOL ISCM strategy at the enterprise and system level and ensure DOL systems have an implemented system-level continuous monitoring strategy.

FINDING 13: SECURITY CONTROLS ASSESSMENTS WERE NOT PERFORMED

The annual security control assessments for 30 systems were not completed in FY 2021, as indicated in email evidence provided by the OCIO. Specifically, 5 of 20 systems that we tested for the FY 2021 FISMA performance audit did not have security control assessments performed within the past year. The OCIO informed us that the risk to not perform the security control assessments was accepted. However, the OCIO did not formally obtain a risk waiver as required per DOL's Enterprise Risk Management Strategy (ERMS). We were informed that the security control assessments could not be performed timely due to issues establishing contracts with security control assessors.

For one system tested, the security control assessment and corresponding security assessment plan was not completed in FY 2021. Management stated it did not prioritize completing the security control assessment for this system. Instead, management focused resources on transitioning the agency to a remote work environment in reaction to the COVID-19 pandemic.

The DOL CSH states that agencies are required to perform annual security control assessments independent of the security authorization process. All controls employed in an information system are to be assessed throughout the authorized period.

This occurred due to inadequate management by OCIO personnel responsible for ensuring security control assessment were performed as required.

The purpose of a security control assessment is to identify weaknesses and deficiencies and provide essential information needed to make risk-based decisions as part of security authorization processes and ensure compliance to vulnerability mitigation procedures. Failure to complete an annual security control assessment could result in threats and vulnerabilities going overlooked, which can result in an increased risk to the confidentiality, integrity, and availability of DOL information systems and data.

We recommend the CIO:

15. Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of security control assessments.

RECOVER – CONTINGENCY PLANNING

FINDING 14: CONTINGENCY TESTING WAS NOT COMPLETED OR RESULTS NOT DOCUMENTED

For one system tested, management did not perform the CP test within the required annual frequency, per the CSH. Management stated that it did not prioritize CP testing. Instead management focused its resources on transitioning the agency to a remote work environment in reaction to the COVID-19 pandemic.

For one system tested, the CP test after action report did not address the following:

- Notification procedures,
- Restoration of normal operations. and
- Other plan testing (where coordination is identified, such as DOL Continuity of Operations Plan [COOP] and Business Continuity Plan [BCP]).

The CSH states the CP must be tested at least annually using agency-defined tests and exercises to determine the plan's effectiveness and the agency's readiness to execute the plan. Also, CP testing must be coordinated with agency elements responsible for related plans, e.g., the BCP, Disaster Recovery Plan (DRP), COOP, and Incident Response Plan (IRP). Also, the CP test should utilize a variety of test elements, to include notification drills, component tests of the backup process, tabletop exercises, and functional exercises to include testing of hot/warm/cold sites.

Additionally, NIST SP 800-34, Rev. 1, states the following areas should be addressed in a contingency plan test, as applicable:

- Notification procedures,
- System recovery on an alternative platform from backup media,
- Internal and external connectivity,
- System performance using alternate equipment,
- Restoration of normal operations, and
- Other plan testing (where coordination is identified, e.g., COOP and BCP).

This occurred due to inadequate oversight by the OCIO personnel responsible for ensuring contingency planning tests were completed as well as a lack of adequate resources at the system level to perform the testing.

The purpose of performing a CP test is to determine the effectiveness of the plan and the agency's readiness to execute the plan. The failure to conduct a thorough contingency plan test could lead to an increased risk that potential weaknesses are not identified in the plan; therefore, corrective actions are not taken to maintain an effective plan.

We recommend the CIO:

16. Implement changes in operations, management and oversight that enforces DOL requirements for the timely completion of contingency plan tests.

FINDING 15: INDIVIDUALS DID NOT RECEIVE REQUIRED ANNUAL CONTINGENCY PLAN TRAINING

For three systems tested, individuals with CP roles and responsibilities did not complete an annual refresher training. Specifically, we noted the following:

- For one system tested, two of five selected individuals with CP responsibilities did not complete annual CP training. A CP refresher training was held for all individuals with CP roles and responsibilities associated with the system tested. However, two of the individuals selected for testing were unable to take the training and did not attend an alternative session to meet the requirement. Due to lack of management oversight, these individuals were not held accountable to take the required training.

- For another system tested, one of two selected individuals with CP responsibilities did not complete annual CP training. Management stated that the individual in question did not receive the invitation to attend the training due to lack of oversight.

- For another system tested, two of two selected individuals with CP responsibilities did not complete annual CP planning training. Management stated that it did not prioritize performance of CP controls. Instead, management focused its resources on transitioning the agency to a remote work environment in reaction to the COVID-19 pandemic.

The DOL CSH states personnel shall receive training within 90 days of assuming a system CP role or responsibility and must attend a refresher training at least annually.

These issues arose due to inadequate management oversight by the OCIO personnel responsible for ensuring employees responsible for contingency planning activities are properly trained.

By not ensuring those with CP responsibilities are trained periodically, there is an increased risk that, during an adverse event, these individuals may not

appropriately execute their CP duties, which could lead to the systems and operations not being restored effectively.

We recommend the CIO:

17. Enhance the OCIO monitoring of the completion of the required annual training by individuals with CP responsibilities.

FINDING 16: BUSINESS IMPACT ANALYSIS WAS NOT COMPLETED

For one system tested, the business impact analysis (BIA) was in draft form and had not been finalized due to competing management priorities.

The CSH requires that a BIA be completed as part of DOL's information system contingency planning (ISCP) process. NIST SP 800-34, Rev 1, *Contingency Planning Guide for Federal Information Systems* states that the purpose of a BIA "is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption."

This occurred due to inadequate oversight by the OCIO personnel responsible for ensuring security documentation, including the BIA, is complete, accurate and approved by management.

The failure to perform a BIA increases the risk that potential weaknesses are not identified in the ISCP, and, therefore, corrective actions are not taken to maintain an effective ISCP and to integrate it with other related plans.

We recommend the CIO:

18. Enhance the OCIO monitoring and oversight of system owners to complete BIAs.

CONCLUSIONS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, DOL has consistently implemented its information security program and practices for its information systems for the 5 Cybersecurity Functions and 9 FISMA Metric Domains. We identified findings within 4 of 5 Cybersecurity Functions and 6 of the 9 FISMA Metric Domains based on the procedures we performed related to the 20 selected information systems for review along with entity-wide testing procedures. Based on the CyberScope results, DOL's information security program was assessed as not effective because a majority of the FY 2021 IG FISMA Reporting Metrics were rated Consistently Implemented (Level 3). We assessed DOL's information security program and practices for its information systems as not effective based on the calculation performed in CyberScope.

We issued 16 findings and made 18 recommendations related to these control deficiencies that should strengthen DOL's information security program if effectively addressed by management. The root causes that led to the control deficiencies identified as part of this performance audit may contribute to control deficiencies for other systems outside of the scope of this audit. Additionally, we identified that for 18 of the 45 NoFs issued, the root cause of these issues was inadequate management oversight from OCIO to information systems managed outside of OASAM.

In improving and progressing the maturity of the DOL information security program, the CIO should consider applying these recommendations to its entire universe of systems. And for information systems managed outside of OASAM, the CIO should consider performing a review of all such systems to assess their compliance with DOL's information system policies and 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 generally concurred with our findings and recommendations and provided planned corrective actions that were responsive to the intent of our recommendations (see Management Response).

AGENCY COMMENTS - MANAGEMENT'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

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

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA Digitally signed by GUNDEEP AHLUWALIA Date: 2022.01.05 17:38:14 -05'00'

SUBJECT: Management Response to the DRAFT REPORT - (Fiscal Year) *FY 2021 FISMA DOL Information Security Continuous Monitoring Controls Remain Deficient Report*, Report Number: 23-22-001-07-725

This memorandum responds to the above-referenced Draft Report – (Fiscal Year) *FY 2021 FISMA DOL Information Security Continuous Monitoring Controls Remain Deficient Report*, issued December 15, 2021. Cybersecurity continues to be a top priority at the Department, and DOL leadership remains committed to continuously strengthening DOL's cybersecurity posture. DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve upon within the cybersecurity program.

Management generally concurs with the findings identified during the FY 2021 FISMA audit evaluation and described in the draft report. In all cases, we have either since addressed the associated recommendations or have developed plans to address them in FY 2022. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).

During FY 2021, the Department took several actions to strengthen DOL's cybersecurity program, including in areas prioritized under Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021). For example, the Department developed a roadmap for Zero Trust, enhanced policy and procedure for Secure Supply Chain, and continued implementing enterprise-wide solutions to enhance encryption, multifactor authentication, IT asset management, incident response and incident monitoring. The Department continued deployment of additional Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) tools for vulnerability management, implementation of new Data Loss Prevention mechanisms, and transition of FISMA systems due for periodic reauthorization into Ongoing Authorization. Moreover, DOL provided additional risk-based security and privacy awareness trainings – including quarterly phishing exercises -- to address increased cybersecurity risks faced by remote users. In the areas of incident detection and response, DOL successfully deployed its Vulnerability Disclosure Program and enhanced its 24x7 Security Operations Center (SOC) to substantially reduce critical vulnerabilities within the Department.

DOL achieved the following positive cybersecurity results during FY 2021:

- Met all 10 of the President's Management Agenda (PMA) Cross-Agency Priority (CAP) Cybersecurity goals.
- Maintained the highest rating of "Managed Risk" across all measured function areas in the FY 2021 Risk Management Assessment (RMA) portion of the CIO FISMA report.
- Closed 12 previously open cyber-related OIG findings from previous years.
- Made the following improvements based on OIG recommendations:

  - Established a comprehensive inventory of web applications, developed a process, and distributed guidance to maintain the inventory centrally in order to better protect DOL's web applications from external threat.
  - Provided awareness training for multiple function areas, such as third-party continuous monitoring, identity and access management, and patch management.
  - Continued to improve POA&M oversight with updated procedures and reporting, providing leadership with a better view of cybersecurity risks.
  - Implemented SECURE Technology Act requirements to address organizational cyber supply chain risk.
  - Developed processes to ensure data backups are monitored for successful completion and that actions are taken timely to resolve data backup failures.
  - Improved PIV card processes by developing and implementing a system that maintains and tracks the employment status of DOL contractors with PIV cards and automatically notifying the appropriate stakeholders when contractors are separated to provide appropriate access control.
  - Developed and implemented a new enterprise-wide cybersecurity risk management strategy and program, aligned with NIST SP 800-39 and NIST SP 800-53, Rev. 4.
- Improved the FISMA OIG-determined maturity level in 6 of the 57 (11 percent) individual control areas compared to FY 2020, resulting in 20 of 57 (35 percent) areas rated as *Effective* (Level 4 or Level 5), including three areas rated at the highest level of *Optimized*.

Looking ahead, DOL will continue to focus on strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. The Department intends to:

- Continue to improve in the adoption of multifactor authentication and encryption of data-at-rest and in-transit;
- Reinforce and improve in the 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;
- Continue its enhancement of DOL's information security continuous monitoring (ISCM) capability by implementing key performance indicators (KPIs) at the Enterprise-, Mission/Business Process-, and System-level, and implementing DHS' recently updated CDM agency-level dashboard; and
- Continue SOC enhancements that will allow the Department to anticipate and mitigate risk, and stay 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 (CISO), at Blahusch.Paul.E@dol.gov or (202) 693-1567. As the CISO, Paul Blahusch is the responsible party for the corrective actions identified in this correspondence.

cc: Rachana Desai Martin, Assistant Security for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
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 (ISSP)

APPENDIX A: GLOSSARY

ACRONYM	DEFINITION
AICPA	American Institute of Certified Public Accountants
AO	Authorizing Official
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CCM	Configuration Change Management
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
COVID-19	Coronavirus Disease 2019
CP	Contingency Planning
CSAM	Cybersecurity Assessment Management
CSH	Computer Security Handbook
CSP	Cloud Service Provider
DSH	Department of Homeland Security
DOL	United States Department of Labor
DPP	Data Protection and Privacy
DRP	Disaster Recovery Plan
ERMS	Enterprise Risk Management Strategy
FIPS	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
IAL/AAL	Identity Proofing and Authentication Processes
IAM	Identity and Access Management
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IR	Incident Response
ISA	Interconnection Service Agreement
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
ISSO	Information System Security Officer

ACRONYM	DEFINITION
IRP	Incident Response Plan
IT	Information Technology
KPMG	KPMG LLP
MP	Media Protection
NIST	National Institute of Standards and Technology
NoF	Notice of Findings
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
Rev	Revision
RM	Risk Management
RMF	Risk Management Framework
ROB	Rules of Behavior
SC	System and Communication Protection
SCRM	Supply Chain Risk Management
SIA	System Impact Analysis
SIEM	Security Information and Event Management
SP	Special Publication
SSP	System Security Plan
ST	Security Training
US-CERT	United States Computer Emergency Readiness Team

APPENDIX B: NOF REFERENCE

Finding #	Function	Domain	NFRs
1	Identify	Risk Management	FISMA-21-41
2	Identify	Supply Chain Risk Management	FISMA-21-18 FISMA-21-42
3	Protect	Configuration Management	FISMA-21-01 FISMA-21-29 FISMA-21-34 FISMA-21-36
4	Protect	Configuration Management	FISMA-21-15
5	Protect	Configuration Management	FISMA-21-05 FISMA-21-26 FISMA-21-37 FISMA-21-38
6	Protect	Configuration Management	FISMA-21-45 FISMA-21-46 FISMA-21-47
7	Protect	Identity and Access Management	FISMA-21-30
8	Protect	Identity and Access Management	FISMA-21-03 FISMA-21-10 FISMA-21-12 FISMA-21-14 FISMA-21-20 FISMA-21-43
9	Protect	Identity and Access Management	FISMA-21-09 FISMA-21-13 FISMA-21-19 FISMA-21-27
10	Detect	Information Security Continuous Monitoring	FISMA-21-02
11	Detect	Information Security Continuous Monitoring	FISMA-21-04 FISMA-21-06 FISMA-21-07 FISMA-21-17 FISMA-21-23 FISMA-21-25 FISMA-21-28 FISMA-21-33
12	Detect	Information Security Continuous Monitoring	FISMA-21-11 FISMA-21-21
13	Detect	Information Security Continuous Monitoring	FISMA-21-22 FISMA-21-32

Finding #	Function	Domain	NFRs
14	Recover	Contingency Planning	FISMA-21-24 FISMA-21-44
15	Recover	Contingency Planning	FISMA-21-08 FISMA-21-31 FISMA-21-35
16	Recover	Contingency Planning	FISMA-21-40

APPENDIX C: STATUS OF PRIOR-YEAR FINDINGS

As part of this year's FISMA Performance Audit, we followed up on management's corrective actions to remediate prior-year findings. We evaluated the corrective actions to determine whether the recommendations were implemented, and the conditions and causes were addressed by management. If there was evidence that the recommendations had been sufficiently implemented, we determined that the recommendation was closed. If there was evidence that the recommendations had been only partially implemented or not implemented at all, we determined the recommendations remained open. Based on our testing, we determined 11 recommendations were closed.

The table below describes the progress that DOL has made in closing prior-year recommendations.

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
RM	FY 2020	Complete, approve, and implement its Enterprise Architecture and related artifacts.	Open
ISCM	FY 2019	Update the ISCM strategy guide with current ISCM performance metrics.	Open
RM	FY 2020	Work with DOL management to update the DOL cybersecurity risk management strategy so that it appropriately addresses each activity and task described in NIST SP 800-39 and NIST SP 800-53, Rev. 4, PM-9, Risk Management Strategy.	Closed
ISCM	FY 2020	Update their ISCM plan to include 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.	Closed
ISCM	FY 2018	Monitor the agencies' ongoing progress to ensure that established procedures and controls are operating effectively	Closed
RM	FY 2018	Conduct a risk assessment to identify the root causes of the identified deficiencies	Closed

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
RM	FY 2018	Coordinate efforts among the DOL agencies to design and implement procedures and controls to address account management, system access settings, configuration management, system audit log configuration and reviews, and patching and vulnerability management control deficiencies in key financial feeder systems.	Closed
IAM	FY 2019	Design and implement controls to perform and document a periodic review of audit logs that report privileged user activity.	Open
CP	FY 2019	Develop and implement contingency planning performance metrics.	Open
RM	FY 2019	Perform a reconciliation of the current state of each DOL information system and the related classification to the information documented for each system in Cyber Security Assessment and Management and reconcile any differences.	Closed
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
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
ISCM	FY 2020	Implement a process to review the latest NIST SPs and update the appropriate DOL documentation consistent with the new standards and best practices put forth by NIST.	Closed
CM	FY 2020	Develop, define, implement, and monitor change management key performance indicators that align DOL's goals and objectives.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
IR	FY 2020	Provide additional resources to support operational activities during unforeseen circumstances.	Open
CM	FY 2020	Update the patching process to ensure patches are applied within appropriate timeframes.	Closed
IAM	FY 2020	Provide training on removing access for separated DOL employees to all DOL officials in the oversight role.	Closed
RM	FY 2020	Review, revise as necessary, finalize, and implement their revised SDLC Manual.	Closed
CM	FY 2020	Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process.	Open
RM	FY 2020	Review NIST SP 800-160 Vol. 1 and 2 and update the CSH to integrate security engineering principles, as appropriate.	Closed
IAM	FY 2020	Provide training over the application user activity review process.	Open
RM	FY 2018	Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies that have been communicated to DOL management.	Open
ISCM	FY 2018	Develop and implement performance metrics that will be used to manage and measure the effectiveness of the DOL information security program.	Open
CM	FY 2019	Design and implement controls to monitor DOL assets for missing patches, service packs, hot fixes, and other software updates that are not associated with a CVE.	Open
DPP	FY 2019	Implement data encryption configurations/solutions at the server level for data at rest for PII.	Open
CM	FY 2019	Design and implement controls and policies to formally perform and document the periodic review of baseline configuration scans across DOL servers and databases.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
RM	FY 2019	Implement technologies for both DOL and the Bureau of Labor Statistics to detect and prevent unauthorized hardware and software from connecting to the local DOL network.	Open
CM	FY 2019	Develop and implement performance metrics for configuration management.	Open
IAM	FY 2019	Develop and implement access control performance metrics.	Open
CM	FY 2019	Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner.	Open
IAM	FY 2019	Finalize the implementation of the access control technologies.	Open
RM	FY 2020	Validate that the classification of DOL systems is in accordance with policy, and that system interconnections are appropriately documented within its inventory.	Open
IAM	FY 2020	Enforce DOL policies and procedures regarding separation of duties so developers do not possess the ability to migrate changes to production.	Open
CM	FY 2020	Enforce DOL security baseline polices with DOL's CSPs and develop a security configuration checklist for the CSPs.	Open
IAM	FY 2020	Implement policies and procedures regarding user access reviews for tenants that reside on the platform as a service in accordance with requirements outlined in the DOL CSH.	Open
CM	FY 2020	Implement a process for approving deviations from established configuration settings.	Open
IAM	FY 2020	Implement a process for periodic review or monitoring of PIV Exemptions to ensure the process is operating effectively.	Open
RM	FY 2020	Develop sufficiently defined quantitative and qualitative metrics that provide meaningful indications of security status and trend analysis at all risk management tiers.	Open

Related Domain	Report Year	Prior-Year Recommendation	Status of Recommendation
RM	FY 2020	Validate that systems have received either the appropriate classification or risk waiver that would exempt the system from specific security requirements.	Open
IAM	FY 2020	Reinforce the PIV Exemption approval process through training.	Open
IAM	FY 2020	Document the responsibilities of control activities for tenants that reside on the PaaS through policies and procedures that include user activity reviews in accordance with requirements outlined in the DOL policy.	Open
CP	FY 2020	Monitor contingency plan testing and exercises through examination of after-action reviews.	Open

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
Washington, DC 20210