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

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2020 FISMA DOL INFORMATION SECURITY REPORT: PROGRESS NEEDED TO IMPROVE RISK MANAGEMENT AND CONTINUOUS MONITORING INFORMATION SECURITY CONTROLS

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.

Elliot P. Lewis
Assistant Inspector General for Audit

DATE ISSUED: December 22, 2020
REPORT NUMBER: 23-21-001-07-725

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

BRIEFLY...

FY 2020 FISMA DOL INFORMATION SECURITY REPORT: PROGRESS NEEDED TO IMPROVE RISK MANAGEMENT AND CONTINUOUS MONITORING INFORMATION SECURITY CONTROLS

December 22, 2020

WHY OIG PERFORMED THE AUDIT

The U.S. Department of Labor (DOL) spends approximately $666 million annually on its Information technology (IT) assets that support the programs needed to fulfill DOL's mission. As IT plays an integral role in providing the services and operations needed to fulfill DOL's mission, it is imperative that DOL maintain a strong IT security program to protect these assets. Ineffective information security programs increase the risk of unavailable service, security breaches, and unreliable information. Under the Federal Information Security Modernization Act of 2014 (FISMA), Inspectors General are required to perform annual independent evaluations of their agency's information security program and practices.

WHAT OIG DID

We contracted with KPMG LLP to conduct an independent audit of DOL's Fiscal Year (FY) 2020 information security program, for the period October 1, 2019, to September 30, 2020. KPMG partly based its determinations on tests of a selection of DOL's entity-wide security controls and system-specific security controls across 20 DOL information systems.

READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2021/23-21-001-07-725.pdf

WHAT THE AUDIT FOUND

KPMG reported 18 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. As a result of the issues identified, the Department of Homeland Security's (DHS) FISMA reporting system determined DOL's information security program was not effective for FY 2020.

To be considered an effective information security program, DHS requires implementation of security controls to a level identified as "Managed and Measurable" for a majority of the cybersecurity functions. While the results determined DOL's information security program had achieved a level of consistently implemented for all 5 cybersecurity functions, the weaknesses identified demonstrated that the program had not achieved the level of managed and measurable in 3 of the 5 cybersecurity functions: Identify, Detect and Recover.

Additional progress is needed in 3 of its domains: Configuration Management, Identity and Access Management, and Data Protection and Privacy. These domains within the Protect Function did not fully achieve the Managed and Measurable rating and will need to be a focus of DOL in order to maintain the overall rating.

The information security program's scores showed some improvements from FY 2019, which may indicate the adoption and implementation of new tools to address the issues previously identified. However, based on the issues identified, we remain concerned about the continued improvements 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 25 recommendations to improve DOL's information security program, including establishing performance metrics. Management generally concurred with the findings and recommendations identified and described in our report. OCIO stated it has addressed or has developed plans to address all recommendations.

U.S. Department of Labor

Office of Inspector General
Washington, D.C. 20210

INSPECTOR GENERAL'S REPORT

Gundeep Ahluwalia
Chief Information Officer
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

The U.S. Department of Labor's (DOL) Office of Inspector General (OIG) contracted with KPMG LLP to conduct an independent audit of DOL's Fiscal Year (FY) 2020 information security program. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal Inspectors General, or an independent external auditor, to conduct annual evaluations of the information security program and practices of their respective agencies.

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, 2019, to September 30, 2020. The determinations in this report were based, in part, on the testing of a selection of DOL's entity-wide security controls and system-specific security controls across 20 of its information systems. Additional details regarding the scope of the independent audit are included in Appendix A of KPMG's attached report.

RESULTS

KPMG reported 18 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 produced 36 findings 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 2020. To be considered an effective information security program, DHS requires implementation of security controls to a level identified as "Managed and Measurable" for a majority of the cybersecurity functions. While results determined DOL's information security program had achieved a level of consistently implemented for all 5 cybersecurity functions, the weaknesses identified demonstrated that the program had not achieved the level of managed and measurable in 3 of the 5 cybersecurity functions: Identify, Detect and Recover.

Although Office of Chief Information Officer (OCIO) received a Managed and Measurable (Level 4) rating within the Protect Function, additional progress is needed in 3 of its domains: Configuration Management, Identity and Access Management, and Data Protection and Privacy. The OCIO will need to focus on these domains in order to maintain the overall level of Managed and Measurable for the Protect Function.

Compared to the FY 2019 FISMA assessment, we believe the OCIO improved the accuracy of self-assessments of its information security progress. However, based on outstanding issues, we remain concerned about the uneven oversight and accountability of DOL's information security program.

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

Elliot P. Lewis
Assistant Inspector General for Audit

U.S. Department of Labor Federal Information Security Modernization Act of 2014 Fiscal Year 2020 Performance Audit

December 22, 2020

KPMG LLP
8350 Broad Street, Suite 900
McLean, VA 22102

Table of Contents

INDEPENDENT PERFORMANCE AUDIT ON THE EFFECTIVENESS OF THE U.S. DEPARTMENT OF LABOR'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT 1

BACKGROUND 4

Agency Overview *4*

Federal Information Security Modernization Act *4*

FISMA Inspector General metrics and reporting *5*

OVERALL RESULTS 6

Identify – Risk Management *7*

Protect – Configuration Management *8*

Protect – Identity and Access Management *9*

Protect – Data Protection and Privacy *10*

Protect – Security Training *10*

Detect – Information System Continuous Monitoring (ISCM) *11*

Respond – Incident Response *11*

Recover – Contingency Planning *12*

FINDINGS 13

Identify – Risk Management 13

Finding 1: Risk Management Strategy *13*

Finding 2: Enterprise Architecture *14*

Finding 3: Weakness in Security Engineering Principles *14*

Finding 4: Third-Party Monitoring *15*

Finding 5: Weakness in the System Inventory *16*

Protect – Configuration Management 17

Finding 6: Change Management Performance Measurements 17

Finding 7: Change Management Separation of Duties 17

Finding 8: Common Secure Configurations 18

Finding 9: Flaw Remediation 19

Protect – Identity and Access Management 20

Finding 10: Personal Identity Verification (PIV) Card Authentication Enforcement 20

Finding 11: Account User Review 21

Finding 12: Use Notification Message 22

Finding 13: Session Lock/Termination 23

Finding 14: Personnel Termination 24

Finding 15: Audit Log Review 24

Detect – Information Security Continuous Monitoring 25

Finding 16: Weakness in DOL's ISCM Plan 25

Recover – Contingency Planning 27

Finding 17: Lack of after-action review performed for contingency plan test results 27

Finding 18: No Contingency Plan Test Performed 27

MANAGEMENT'S RESPONSE TO THE REPORT 29

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY 31

APPENDIX B: GLOSSARY 34

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

INDEPENDENT PERFORMANCE AUDIT ON THE EFFECTIVENESS OF THE U.S. DEPARTMENT OF LABOR'S INFORMATION SECURITY PROGRAM AND PRACTICES REPORT

Chief Information Officer and Acting Inspector General
Department of Labor
200 Constitution Avenue
Washington, DC 20405

This report presents the results of our independent performance audit of the U.S. Department of Labor's (DOL) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including DOL, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the U.S. Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (FY 2020 IG FISMA Reporting Metrics) to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor to perform the independent evaluation as determined by the IG. DOL Office of Inspector General (OIG) contracted KPMG LLP (KPMG) to conduct this independent performance audit and monitored our work to ensure we met professional standards and contractual requirements.

We conducted an independent performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and applicable American Institute of Certified Public Accountants (AICPA) standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis to address the audit objectives and support our findings and conclusions.

The objective for this independent performance audit was to assess the effectiveness of DOL's information security program and practices, including DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines for the period October 1, 2019, to September 30, 2020. We based our work on a selection of DOL-wide security controls and a selection of system-specific security controls across 16 selected DOL information systems and 4 DOL contractor information systems.[1] Additional details regarding the scope of our independent performance audit are included in Appendix A, Objective, Scope, and Methodology. Appendix B contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, DOL has consistently implemented its information security program and practices for its information systems for the 5 cybersecurity functions[2] and 8 FISMA metric domains.[3] We identified findings within 4 of 5 cybersecurity functions and 5 of the 8 FISMA metric domains based on the procedures we performed related to the selected 20 information systems for review (16 federal and 4 contractor systems) along with entity-wide testing procedures. Based on the CyberScope[4] results, DOL's information security program was not effective because a majority of the FY 2020 FISMA metrics were rated Consistently Implemented (Level 3).

[1] DOL information systems are operated internally by DOL, whereas contractor systems are operated by a contractor on behalf of the agency.

[2] OMB, DHS, and CIGIE developed, in consultation with the Federal CIO Council, the FY 2020 IG FISMA Reporting Metrics. In FY 2016, the 8 IG FISMA metric domains were aligned with the 5 cybersecurity functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The FY 2020 metrics mark a continuation of the work undertook in FY 2017 when the IG evaluations transitioned into a maturity model approach.

[3] As described in DHS's *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0, April 17, 2020,* the 8 FISMA metric domains are risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

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

CyberScope calculated the level as not effective because only 3 cybersecurity metric domains were assessed at Managed and Measurable (Level 4) and the remaining 5 domains were assessed at the Consistently Implemented (Level 3).

We reported deficiencies impacting specific FY 2020 IG FISMA Reporting Metrics in *Identify* (risk management); *Protect* (configuration management, and identity and access management); *Detect* (information security continuous monitoring [ISCM]); and *Recover* (contingency planning).

In our report, we have provided the Chief Information Officer (CIO) 18 findings[5] and 25 recommendations that, when addressed, should strengthen DOL's information security program. The DOL CIO generally concurred with our findings and recommendations (see Management's Response to the Report, page 30).

KPMG did not render an opinion on DOL's internal controls over financial reporting or over financial management systems as part of this performance audit. We caution that projecting the results of our performance audit to future periods or other DOL information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

December 22, 2020

[5] The 18 findings incorporate 36 system-level and entity-wide findings that we identified during our testing.

BACKGROUND

AGENCY OVERVIEW

DOL's mission 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.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Title III of the E-Government Act of 2002, which was amended in 2014, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA assigns specific responsibilities to agency heads and IGs in complying with its requirements. FISMA is supported by OMB, the agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk, as well as the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies and procedures. OMB has delegated some responsibility to DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, for the operational aspects of federal cybersecurity, such as establishing government-wide incident response

and aggregating the FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security program and practices and to report the evaluation results to OMB.

FISMA INSPECTOR GENERAL METRICS AND REPORTING

The FISMA program areas are outlined in the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0,* and were prepared by DHS's Office of Cybersecurity and Communications Federal Network Resilience. The CyberScope functions and domains are listed in Table 1 below.

Table 1: CyberScope Functions and Domains

Five Cybersecurity Framework Functions	Eight IG FISMA Domains
Identify	Risk management
Protect	Configuration management, identity and access management, data protection and privacy, and security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

Source: FY 2020 Inspector General FISMA Reporting Metrics v4.0

The 5 specific CyberScope functions are described in detail below:

- *Identify.* Develop organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities by identifying and maintaining a hardware and software inventory.

- *Protect*. Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

- *Detect*. Develop and implement appropriate activities to identify a cybersecurity event.

- *Respond*. Develop and implement appropriate activities to take action regarding a detected cybersecurity event.

- *Recover.* Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity event.

The maturity model definitions for the FY 2020 FISMA metric domains are:

- *Level 1 (Ad Hoc)*. An agency lacks a formalized program and performs activities in a reactive manner.

- *Level 2 (Defined)*. An agency has a formalized program with comprehensive policies, procedures, and strategies consistent with NIST standards but fails to implement them consistently organization-wide.

- *Level 3 (Consistently Implemented)*. An agency consistently implements its program but lacks qualitative and quantitative measures and data on its effectiveness.

- *Level 4 (Managed and Measurable)*. An agency uses metrics to measure and manage implementation of its program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

- *Level 5 (Optimized)*. An agency's program is institutionalized, repeatable, self-regenerating, and updated on a near-real-time basis based on changes in mission or business requirements and the changing threat and technology landscape.

OVERALL 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 5 cybersecurity functions and 8 FISMA metric domains. Based on the maturity level that CyberScope calculates, it was determined that DOL's information security program was not effective[6] because only 3 cybersecurity metric domains were

[6] The scoring methodology is described in the DHS' FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 4.0 April 17, 2020, which requires a Managed and Measurable rating (Level 4) to be considered effective as computed by the entries in CyberScope.

assessed at Managed and Measurable (Level 4) and the remaining 5 domains were assessed at the Consistently Implemented (Level 3). We reported deficiencies impacting specific FY 2020 IG FISMA Reporting Metrics in Identify, Protect, Detect, and Recover. See Table 2.

The FY 2020 IG FISMA Reporting Metrics states the following:

> Level 4, *Managed and Measurable*, is considered an effective level of security at the domain, function, and overall program level. Ratings throughout the 8 domains will be determined by a simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating.

Table 2 below depicts the assessed level of security for each functional area.

Table 2: IG FISMA Metric Maturity Level by Functional Area

Cybersecurity Framework Function	Assessed Maturity Level
Identify	Level 3 – Consistently Implemented
Protect	Level 4 – Managed and Measurable
Detect	Level 3 – Consistently Implemented
Respond	Level 4 – Managed and Measurable
Recover	Level 3 – Consistently Implemented

Source: IG CyberScope entries

During FY 2020, we conducted a performance audit of 20 DOL systems and DOL's entity-wide controls, and we identified and reported 18 findings in this report based on 36 notice of findings and recommendations (NFRs) that we issued to the system and entity-wide control owners. The findings were identified in 4 of the 5 FISMA cybersecurity functions and in 5 of the 8 FISMA metric domains. We also evaluated the prior-year recommendations and determined that DOL had closed 7 out of 20 previous recommendations.

IDENTIFY – RISK MANAGEMENT

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 risk that threatens their mission and services, they are able to establish controls and processes to manage and prioritize risk management decisions.

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. Risk management 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 risk management plan and program that has been developed to address the various risks can provide impactful information to an agency information when establishing an information security program based on these documented risk management decisions.

As a result of our audit procedures, we determined DOL has implemented policies and procedures to maintain a complete and accurate inventory of its major information systems, hardware devices, and software devices. We identified weaknesses in DOL's classification of cloud-based major information systems. Additionally, we noted that DOL was still in the process of implementing systems to track hardware and software devices connected to its network on a near real time basis.

DOL has developed an enterprise risk management strategy and implemented policies and procedures in line with its strategy. However, we determined that there were weaknesses regarding the comprehensiveness of the risk management strategy and the monitoring of the effectiveness of the strategy.

PROTECT – CONFIGURATION MANAGEMENT

The objective of the *Protect* function in the cybersecurity framework is to develop and implement appropriate safeguards to ensure the delivery of critical services of 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 configuration management, identity and access management, data protection and privacy, and security training processes.

FISMA requires agencies to develop an information security program that includes policies and procedures to ensure compliance with minimally acceptable system configuration requirements. Configuration management 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. DOL indicated that they are in the process of overhauling their change management process by implementing a new software tool that will provide additional insights and be able to produce metrics and reports for management.

Based on our audit procedures, we determined that DOL has documented performance measures to determine the effectiveness of its configuration management processes; however, we determined that DOL was unable to track these performance measures due to its transition from 1 change management software to another.

We determined DOL has processes to identify the compliance of its information systems to common secure configurations. DOL does not have a formal process to remediate or approve deviations to its established common secure configurations.

Additionally, we determined that vulnerabilities remained open longer than the defined timeframes in DOL's Computer Security Handbook (CSH). However, we determined that DOL has processes in place to remediate critical vulnerabilities communicated to them by DHS within the DHS-defined timeframes. Last, we determined that DOL's monitoring processes were able to evaluate at a high-level the effectiveness of its vulnerability remediation process.

PROTECT – IDENTITY AND ACCESS MANAGEMENT

The Identity and access management function includes the requirement that an agency implement a set of capabilities to ensure that users authenticate to information technology (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).

DOL has developed an ICAM strategy that has defined specific milestones to track its progress. DOL utilizes that ICAM architecture when developing new applications and continues to integrate its legacy applications into its modern ICAM architecture.

DOL is currently in the process of implementing tools that will assist with single sign-on, user management, and controlling privileged access. DOL has implemented strong authentication methods for privileged user access. However, DOL has inconsistently implemented strong authentication procedures for its regular users.

PROTECT – DATA PROTECTION AND PRIVACY

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and protection of improper disclosure of personal privacy and proprietary information. In today's digital world, 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. 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.

KPMG determined DOL has consistently developed and implemented a privacy program for the protection of personally identifiable information (PII) and has implemented security controls to protect PII. However, 1 system containing PII did not prevent unnecessary access to the PII.

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 consistently measures the effectiveness of its privacy awareness training program through feedback received from users that complete the privacy awareness training and phishing exercises.

PROTECT – SECURITY TRAINING

Security training 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.

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 SYSTEM CONTINUOUS MONITORING (ISCM)

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.

To enhance further the government's ISCM capabilities, Congress established the Continuous Diagnostic Monitoring (CDM) program. The CDM program provides 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.

Over the past year, DOL continued the modernization of its IT infrastructure and the implementation of advanced cybersecurity tools. Although DOL has made strides in improving its cybersecurity posture, DOL should enhance its ISCM program to include processes to analyze the data retrieved from the CDM toolset and generate actionable insights into its security posture. The lack of implementing advanced cybersecurity tools inhibits DOL's ability to allocate resources in a risk-based manner and hold relevant stakeholders accountable for carrying out their roles and responsibilities effectively. In addition, we determined DOL has a process to perform ongoing assessments, but does not maintain ongoing authorization for its information systems.

Additionally, DOL should integrate the data from the CDM tools and ISCM program into the risk management program to allow DOL to manage and reduce risks more effectively, based on defined tolerances.

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 incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. FISMA requires each agency to develop, document, and

implement an agency-wide information security program that includes policies and procedures for incident response.

We determined that DOL monitors and analyzes the effectiveness of its incident response policies, procedures, plans, strategies, and technologies through weekly reports that capture incident response activities. DOL utilizes multiple advanced tools to support the incident response processes. These tools feed into DOL's Security Information and Event Management (SIEM) tool to give a centralized view of the activities. However, DOL does not utilize profiling techniques to maintain a comprehensive baseline of network operations and expected data flows for users and systems.

DOL consistently 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. In addition, 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 contingency planning processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event.

During our audit, we determined that DOL management had consistently implemented its contingency planning procedures, but had not implemented contingency planning performance metrics to achieve a managed and measurable contingency planning program.

FINDINGS

The following provides the details to the 18 individual findings issued to the CIO. These findings are grouped by FISMA metric domain within each cybersecurity function and include related recommendations.

IDENTIFY – RISK MANAGEMENT

FINDING 1: RISK MANAGEMENT STRATEGY

NIST Special Publication (SP) 800-53 Rev.4, *Security and Privacy Controls for Federal Information Systems and Organizations,* states:

> The organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems and implements the risk management strategy consistently across the organization.

Further guidance for developing such a risk management strategy is detailed in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

DOL has not defined a comprehensive risk management strategy to manage risk or information security risk tolerance. DOL's Risk Management process does not allow for the identification and response of information security risks outside of instances in which an agency cannot implement a CSH policy and/or standard. Further, DOL has not implemented a strategy for monitoring the effectiveness of, and changes to, its risk management program. DOL management did not agree with this finding; however, it stated that it will address more explicitly the criteria found in NIST SP 800-39 and NIST SP 800-53, Rev. 4, in future revisions to the strategy.

A comprehensive risk management strategy should define how information system security risk is managed across the organization. This is accomplished by addressing risk at the enterprise, mission, business process, and information system level.

Without a comprehensive risk management strategy, DOL is unable to reduce its information security risk to a tolerable level and ensure that its risk stays within its tolerance over time.

1. We recommend the CIO 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.

FINDING 2: ENTERPRISE ARCHITECTURE

OMB A-130 states:

> Agencies shall develop an enterprise architecture that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture…The [enterprise architecture] should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency, and laying out a plan for transitioning from the current state and future state of the agency, helps agencies to eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among Government, industry, and citizens.

Due to resource constraints, DOL management stated that it was unable to complete, approve, and implement its Enterprise Architecture.

A fully realized enterprise architecture would align DOL's IT infrastructure with its organizational business goals. Failure to maintain a formal enterprise architecture could lead to inefficiencies, performance gaps, and risks related to resource management, acquisitions, and project implementation. Further, this could result in disparate systems and technology introducing unique security risks and vulnerabilities.

2. We recommend the CIO complete, approve, and implement its Enterprise Architecture and related artifacts.

FINDING 3: WEAKNESS IN SECURITY ENGINEERING PRINCIPLES

NIST SP 800-53, Rev. 4, Control SA-8 *Security Engineering Principles,* states that the organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Due to competing priorities and resource constraints, OCIO management informed us that it was unable to update the CSH to reflect the updated NIST SP 800-160 Volume 1 and Volume 2 over security engineering principles. In addition, due to DOL's transition to a shared services model, priorities shifted and DOL has been unable to revise and approve the Software Development Life Cycle (SDLC) manual to include its use of agile development methodology and mobile application development considerations.

Security engineering principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities is constructed. Without defined security engineering principles in line with best practices provided by NIST, the risk increases that systems engineered by DOL do not create trustworthy, secure, and cyber-resilient information systems.

We recommend the CIO:

3. 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.

4. Review NIST SP 800-160 Vol. 1 and 2 and update the CSH to integrate security engineering principles, as appropriate.

5. Review, revise as necessary, finalize, and implement their revised SDLC Manual.

FINDING 4: THIRD-PARTY MONITORING

The DOL CSH requires use of a monitoring checklist to examine the risk associated with DOL's external information systems and to determine if the third-party provider is operating in a manner consistent with DOL's requirements, as defined in the DOL CSH.

For 1 cloud service provider (CSP), DOL did not complete the mandatory continuous monitoring checklist for 3 of the months selected for testing, as the information system security officer (ISSO) was unaware of the updated guidelines over third-party monitoring.

The purpose of conducting a third-party continuous monitoring checklist is to examine the risk associated with the external information systems and to determine if the third-party provider is operating in a manner consistent with the agency's requirements. Failure to conduct the review appropriately could lead to

an increase in undetected risks, which, in turn could negatively impact the integrity, confidentiality, and security of DOL data.

6. We recommend the CIO provide training to responsible personnel over the third-party continuous monitoring review checklist.

FINDING 5: WEAKNESS IN THE SYSTEM INVENTORY

The DOL CSH policy requires that both non-cloud contractor systems and Software as a Service (SaaS) systems be classified as contractor-operated systems, while all other systems should be classified as government systems, such as a system being maintained on a contractor Platform as a Service (PaaS). DOL policy also requires that each information system interconnection be documented.

We found that DOL had misclassified 2 systems as contractor-operated systems rather than as government systems. Management informed us that the Agency Head or Authorizing Official did not appropriately interpret the policy due to the ambiguities with cloud computing platforms. Further, 1 ISSO did not properly document 1 system's interconnections with other information systems in the System Security Plan (SSP) due to management oversight.

Senior DOL management relies on the information provided in the inventory listing to perform strategic planning activities, to fulfill daily operational decisions, and to meet federal reporting guidelines. Without maintaining an accurate classification of information systems, DOL runs the risk that the needs and requirements of an information system may go overlooked. For example, personnel may be unaware of which controls are DOL's responsibility and which responsibilities are for the vendor. The result can be an increased risk to the integrity, confidentiality, and availability of DOL's data contained within the information system.

7. We recommend the CIO validate that the classification of DOL systems is in accordance with policy, and that system interconnections are appropriately documented within its inventory.

PROTECT – CONFIGURATION MANAGEMENT

FINDING 6: CHANGE MANAGEMENT PERFORMANCE MEASUREMENTS

DOL's Change Management Plan documents several key performance indicators, including but not limited to Request for Change aging, unauthorized changes, and percentage of changes that result in an incident, in order to determine the effectiveness of the plan. Additionally, NIST SP 800-55, Rev 1, provides program-level guidelines for quantifying information security performance in support of organizational strategic goals.

DOL management did not track, monitor, and review key performance indicators documented in DOL's Configuration Management Plan for 1 system. During the audit period, the change request system, Remedy, was being decommissioned and ServiceNow Change Management was being implemented. Due to this transition, Remedy reporting functions were discontinued.

Performance measures facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of relevant performance-related data. Without performance measures to gauge the effectiveness of its change management practices, DOL may not be able to detect ineffective change and configuration management policies, procedures, and control activities. This may lead to the loss of the confidentiality, integrity, and availability of DOL information systems.

8. We recommend the CIO, in accordance with DOL Change Management Plan and NIST SP 800-55, Rev. 1, develop, define, implement, and monitor change management key performance indicators that align DOL's goals and objectives.

FINDING 7: CHANGE MANAGEMENT SEPARATION OF DUTIES

The DOL CSH states that systems are required to separate duties of general and privileged users, as necessary, to prevent malicious activity without collusion.

For 1 system tested, a developer migrated a change into the production environment in violation of the DOL CSH separation of duties control requirements. DOL management stated that the development team was unaware of the applicable DOL procedures that they were required to follow.

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malicious activity. Failure to enforce appropriate separation of duties can lead to an increased risk of undetected malicious or unauthorized changes in the production environment or production data.

9. We recommend the CIO enforce DOL policies and procedures regarding separation of duties so developers do not possess the ability to migrate changes to production.

FINDING 8: COMMON SECURE CONFIGURATIONS

The DOL CSH requires DOL agencies establish and implement configuration settings for information technology products employed within the information system. These settings must use agency-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements. Additionally, any deviations from the established configuration settings must be identified, documented and approved.

For 1 CSP, DOL did not document their security baseline, as DOL management stated that it was unaware of their responsibility to document and follow a security baseline. For 22 servers selected for testing, DOL did not implement their common secure configurations. DOL identified deviations from its common secure configurations and did not approve the deviations. The process of reviewing and validating specific deviations to the baseline has not been formalized.

Common secure configurations provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information systems and instructions for configuring those information systems to meet operational requirements set by DOL. A formal process to approve and remediate deviations from established configuration settings allows for the acceptance of risk of deviations where operationally required as well as the implementation of the established configuration settings for the other deviations.

The failure of a process to approve deviations could lead to an increased risk of unauthorized changes to the settings, which could result in a compromise of the integrity, confidentiality, and security of DOL's information systems.

We recommend the CIO:

10. Enforce its security baseline polices with DOL's CSPs and develop a security configuration checklist for the CSPs.

11. Implement a process for approving deviations from established configuration settings.

FINDING 9: FLAW REMEDIATION

The DOL CSH 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 72 hours of release.

b. Updates identified as high importance must be installed within 5 business days of release.

c. Updates identified as moderate importance must be installed within 10 business days of release.

d. Updates identified as low importance must be installed within 20 business days of release.

For 1 system, the database was not patched within the DOL's defined remediation timeframe. This was due to the COVID-19 pandemic, as management put all maintenance activities on hold to ensure there were no outages when personnel were required to stay quarantined. Once activities resumed, ongoing resource limitations caused additional delay in the patch installation.

We identified 39 critical vulnerabilities, 25 high vulnerabilities, 19 moderate vulnerabilities, and 1 low vulnerability that were not patched in accordance with the DOL policy. These vulnerabilities were not patched within the timeframes specified in the DOL policy because the current process does not allow for deploying patches and associated requirements fast enough to meet the timeframes defined in DOL's policy.

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:

12. Provide training to responsible personnel addressing the new guidance for operational activities, including the patch management process.

13. Provide additional resources to support operational activities during unforeseen circumstances.

14. Update the patching process to ensure patches are applied within appropriate timeframes.

PROTECT – IDENTITY AND ACCESS MANAGEMENT

FINDING 10: PERSONAL IDENTITY VERIFICATION (PIV) CARD AUTHENTICATION ENFORCEMENT

With respect to Multifactor Authentication, the DOL CSH requires PIV cards to be the second level of identity verification for all full time DOL users. DOL's Standard Operating Procedure (SOP) states that permanent PIV card logon exemptions may be provided to users that receive agency approval via their agency ISSO.

DOL policy requires that all users authenticate to the network using their PIV credential and unique personal indentation number (PIN). DOL has a process to allow users to login to the network with username and password where it is not practical for the user to login with a PIV card. The control over PIV exemptions was not operating effectively, as PIV exemption approval forms were unable to be provided for 15 out of the 25 users due to lack of management oversight. Additionally, management informed us that the approval process for PIV exemptions was not formally documented.

PIV cards provide multifactor authentication to federal IT resources and facilities, unless users are deemed exempt through formal approval in accordance with agency guidelines. Failure to document and retain PIV exemption approvals could result in unwarranted or unnecessary issuances of PIV exemptions. This could lead to an increased risk of unauthorized access to the DOL network and information systems, which could result in a compromise of the integrity, availability, and confidentiality of DOL data.

We recommend the CIO:

15. Reinforce the PIV Exemption approval process through training.

16. Implement a process for periodic review or monitoring of PIV Exemptions to ensure the process is operating effectively.

FINDING 11: ACCOUNT USER REVIEW

The DOL CSH requires information system accounts be reviewed routinely to ensure that terminated or transferred individuals do not retain system access. Specifically, non-privileged user accounts should undergo quarterly review, while privileged user accounts require a monthly review.

The control over user access review did not operate as designed during the period. Specifically:

- For 2 systems, management could not provide supporting documentation evidencing its review of application privileged user access;

- For 1 system, management could not provide supporting documentation evidencing its review of application non-privileged user access;

- For 3 systems, management could not provide supporting documentation evidencing its review of application privileged and non-privileged user access; and

- For 1 system, the control over review of access for system administrators and database administrators was not performed at the required frequency.

For 2 systems that reside on a PaaS, responsible personnel were unclear as to who had responsibility to conduct the review. For 2 systems, management was unaware of the required frequency for user reviews. For another system, management misunderstood the frequency in which the review needed to be performed and the review was performed at a lesser frequency. Additionally, for 2 systems, DOL did not perform the user reviews appropriately and as prescribed due to resource constraints.

Periodic review of accounts helps ensure adherence to account management requirements. Failure to conduct periodic reviews of user account access could

result in unauthorized access to the systems, users performing functions that do not match their job descriptions, and potential segregation of duties conflicts not being detected and prevented timely. These issues increase the risk of compromise to the confidentiality, integrity, and availability of DOL data and other sensitive information.

We recommend the CIO:

17. 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.

18. Provide additional resources to support the security requirements and a training over the application user access review process, as documented in the DOL CSH.

FINDING 12: USE NOTIFICATION MESSAGE

The DOL CSH requires that the information system must display an approved privacy and security notification message or banner to users before granting them access, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance that state:

a. Users are accessing a U.S. Government information system

b. Information system usage may be monitored, recorded, and subject to audit

c. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

d. Use of the system indicates consent to monitoring and recording

Additionally, the DOL CSH requires the information system to display the notification messages on the screen until the user acknowledges the usage conditions and takes explicit actions to log onto or further access the information system.

One system did not implement the “use notification message or banner” before granting system access to users, as management misunderstood the system use notification or banner requirements.

Displaying a “use notification message or banner” prior to system access informs users of the applicable privacy and security notices associated with their use of a U.S. Government information system, consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The failure to provide a use notification message could lead to lack of awareness of user obligations when logged into the system, as well as increase the risk of unauthorized users participating in unauthorized and illegal activity.

We offer no recommendation for the issue because DOL remediated this issue during the FISMA performance audit period, and we were able to determine that management implemented the corrective action.

FINDING 13: SESSION LOCK/TERMINATION

The DOL CSH requires that the information system prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user. Additionally, the information system automatically terminates a user session after 30 minutes of user inactivity.

Controls over the application session lock configurations for 1 system and controls over session timeout configurations for 1 system did not operate as designed during the audit period. Specifically, for 1 system, due to lack of management oversight of the security requirements, the application configurations called for session lockout after 30 minutes of inactivity. For the other system, due to the operational issue, the session timeout configuration was increased to troubleshoot the root cause of the issue. After it was adjusted, it was not adjusted back to be within DOL policy requirements due to lack of management oversight.

A session timeout terminates all processes associated with a user’s session after a specific time of inactivity. A session lock prevents further access to the system after a specific time of inactivity, until the user reestablishes access appropriately. The failure to have compliant session timeout and session lock configurations could lead to an increased risk of unauthorized access.

We offer no recommendation as DOL has remediated this issue during the FISMA performance audit period, and we were able to determine that management implemented the corrective action.

FINDING 14: PERSONNEL TERMINATION

The DOL CSH requires the agency to notify account managers of separated employees to deactivate the associated accounts within 10 business days from the Human Resources (HR) termination effective date (for employees) or Contractor Officer Representative separation date of record (for contractors) when the separation is voluntary. If the separation is involuntary (including as the result of termination due to emergency or hostile situations), the DOL CSH required deactivation within 4 hours.

The controls over the removal of separated employees for 1 system did not operate effectively during the period. Specifically, due to lack of management oversight, 1 separated user retained an active account for 3 months following their separation date.

The purpose of timely removal of access to a system is to ensure that unauthorized users do not retain access after their separation. Without the timely removal of access, there is an increased risk that unauthorized use of the information systems could occur, which increases the risk of compromise to the confidentiality, integrity, and availability of the data residing on the information system.

19. We recommend the CIO provide training on removing access for separated DOL employees to all DOL officials in the oversight role.

FINDING 15: AUDIT LOG REVIEW

The DOL CSH requires management to review and analyze the information system's audit records at least monthly for indications of inappropriate or unusual activity and report any findings to designated agency officials.

During the audit period, review of application privileged user activity for 2 systems did not operate as designed. Specifically, the 2 systems reside on a PaaS and the responsible personnel were unaware that it was, in fact, their responsibility to perform the review.

The purpose of periodic audit log review is to identify suspicious behavior or supporting evidence of such behavior and to ensure that individuals are held accountable for their actions. Failure to periodically review user account activity increases the risk that any anomalous or malicious activity might go unnoticed and uninvestigated. This could also increase the risk of compromise to the confidentiality, integrity, and availability of DOL data.

We recommend the CIO:

20. 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.

21. Provide training over the application user activity review process.

DETECT – INFORMATION SECURITY CONTINUOUS MONITORING

FINDING 16: WEAKNESS IN DOL'S ISCM PLAN

The OMB Circular A-130, Appendix I, section 4, Specific Requirements, states that agencies shall:

> 5) Develop and maintain an ISCM strategy to address information security risks and requirements across the organizational risk management tiers;
>
> 6) Implement and update, in accordance with organization-defined frequency, the ISCM strategy to reflect the effectiveness of deployed controls; significant changes to information systems; and adherence to Federal statues, policies, directives, instructions, regulations, standards, and guidelines;
>
> […]
>
> 8) Establish and maintain an ISCM program that:
>
> a) Provides an understanding of agency risk tolerance and helps officials set priorities and manage information security risk consistently throughout the agency;
>
> b) Includes metrics that provide meaningful indications of security status and trend analysis at all risk management tiers;
>
> […]

g) Maintains awareness of threats and vulnerabilities that have the potential to affect security, including the mitigation of those threats and vulnerabilities.

DOL does not have a procedure to review and update the ISCM strategy and ISCM Program on a defined frequency, nor does it have a policy and procedure for security status monitoring. Further, the ISCM strategy and plan do not define quantitative and qualitative metrics to provide meaningful indications of security status and trend analysis at all risk management tiers. DOL management stated that it has been unable to update its policies to satisfy each task within the NIST SPs due to competing priorities and resource constraints.

Regularly reviewing the ISCM strategy and program helps to ensure that metrics tracked by the strategy and program continue to be relevant, meaningful, actionable, and supportive of risk management decisions throughout the organization. Without procedures to review the ISCM strategy and program, DOL will be unable to ensure that it is operating within acceptable risk tolerance levels that metrics remain relevant, and that data is current and complete. Additionally, failure to have procedures for security status monitoring 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. Lastly, without sufficiently defined quantitative and qualitative metrics, DOL will be unable to convey accurately the security posture of the organization's information and information systems.

We recommend the CIO:

22. 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.

23. Develop sufficiently defined quantitative and qualitative metrics that provide meaningful indications of security status and trend analysis at all risk management tiers.

RECOVER – CONTINGENCY PLANNING

FINDING 17: LACK OF AFTER-ACTION REVIEW PERFORMED FOR CONTINGENCY PLAN TEST RESULTS

The DOL CSH requires that an after-action review of a contingency plan test be performed.

For 2 systems, DOL did not perform an after-action review of the contingency plan test results due to management oversight.

An after-action report following a contingency plan test documents the findings discussed during the debrief, observations made during the test, and lessons learned. Communicating information on the planning and performance of recovery activities to relevant stakeholders and management teams gives them information to make risk-based decisions and to take appropriate action based on the results (for example updating policies and procedures). The failure to document and communicate this information inhibits relevant personnel from making appropriate risk-based decisions and taking necessary after actions, and also leads to a lack of awareness of recovery activities.

24. We recommend the CIO monitor contingency plan testing and exercises through examination of after-action reviews.

FINDING 18: NO CONTINGENCY PLAN TEST PERFORMED

The DOL CSH requires information system contingency plans to be tested on an annual basis.

For 1 system, DOL did not perform a contingency plan test. We were informed the system was in a transitional period and was going to be classified as a minor application at the end of the fiscal year. However, during the year, it was still classified as a major information system, and management did not approve an appropriate waiver to forego a contingency plan test.

The purpose of performing an annual contingency plan test is to determine the plan's effectiveness on organizational operations, assets, and individuals due to contingency operations and the agency's readiness to execute the plan. The failure to perform an annual contingency plan test could lead to an increase in

unidentified potential weaknesses and, therefore, failure to take corrective actions to maintain an effective plan and to integrate with other related plans.

25. We recommend the CIO validate that systems have received either the appropriate classification or risk waiver that would exempt the system from specific security requirements.

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: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA
Digitally signed by GUNDEEP AHLUWALIA
Date: 2020.12.16 15:15:47 -05'00'

SUBJECT: Management Response to the DRAFT REPORT – FY 2020 FISMA DOL Information Security Report, Report Number: 23-21-001-07-725

This memorandum responds to the above-referenced Draft Report - *FY 2020 FISMA DOL Information Security Report*, issued December 10, 2020, for management's review and response.

DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas for improvement within the cybersecurity program. The security of the Department of Labor's information and information systems is one of the Department's top priorities, and we remain committed to ensuring the Department implements the necessary and effective safeguards.

Management generally concurs with the findings and recommendations identified during the FY 2020 FISMA audit evaluation and described in the Draft Report. In all cases, we have either since addressed the recommendation or have developed plans to address it in FY 2021. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of the Inspector General.

To provide a more complete picture of the Department of Labor's cybersecurity program, management wishes to highlight the actions that have taken place within the Department's IT environment to strengthen DOL's cybersecurity posture. These activities include: enhancements to our centralized inventory solution; the implementation of a suite of robust baseline configuration management tools and processes; improvements to our qualitative and quantitative performance measures for our incident response capability; continued trend analysis, metrics gathering, and role-based training as components of our security training; and, development of a continuous monitoring strategy that supports the shift of DOL information systems into ongoing authorizations.

We were pleased that the results of some of our actions were reflected in the report, such as:

- Achieving Level 4 – *Managed and Measurable* in two of five function areas (Protect and Respond) – an improvement from FY 2019 when this was achieved in only one function area (page 7);
- The closure of seven recommendations from the FY 2019 assessment (page 7);
- A vulnerability remediation monitoring process noted as having a high-level of effectiveness (page 9);
- That the Department's identity, credential and access management (ICAM) program has defined milestones, and is now used for new and legacy applications to provide single sign-on, user management, and control privileged access (page 9); and
- DOL – via the Continuous Diagnostic Monitoring (CDM) program - continued the modernization of its IT infrastructure with the implementation of advanced cybersecurity tools (page 11).

In addition, though not noted in the OIG FISMA report, DOL achieved the following positive cybersecurity results during FY20:

- Met or exceeded 9 of 10 (90%) of the President's Management Agenda Cross-Agency Priority Cybersecurity Goals;
- Maintained the highest rating of "Managing Risk" across all measured areas in the FY20 Risk Management Assessment (RMA) portion of the FISMA report;
- Improved the FISMA OIG-determined maturity level in 13 of 59 (22%) individual control areas compared to FY19, resulting in 20 of 59 (34%) areas rated as Effective (Level 4 or Level 5), including two areas rated at the highest level of *Optimized*;
- Closed 23 open OIG findings from previous years (83 IT-related closures over the last three years); and
- Largely completed the IT Shared Services initiative that places Department IT – including cybersecurity – under the direct organizational authority of the CIO.

We appreciate the opportunity to provide input. If you have any questions, please contact me directly at (202) 693-4446 or have your staff contact Paul Blahusch, Chief Information Security Officer, at Blahusch.Paul.E@dol.gov or (202) 693-1567.

cc: Bryan Slater, Assistant Security for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Geoffrey 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: OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective was to determine to what extent DOL has implemented its information security program.

In fulfilling the objective above, we performed a performance audit of DOL's information systems to evaluate the effectiveness of the information security program and the implementation of security controls that include policies, procedures, and practices to determine whether DOL met OMB and FISMA-required information security controls.

NIST SP 800-53, Rev. 4, defines security control effectiveness as the extent that controls are: 1) implemented correctly; 2) operating as intended; and 3) producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies. We tested the NIST 800-53, Rev. 4. controls referenced in the FY 2020 IG FISMA Reporting Metrics. We also performed additional testing of security control areas as required by DHS, OMB, CIGIE, and other oversight organizations.

SCOPE

To accomplish our objective, we evaluated security controls in accordance with applicable legislation, presidential directives, and the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 4.0,* dated April 17, 2020. We reviewed the DOL information security program from a program-level perspective and then examined how each of the information systems selected for our testing implemented these policies and procedures for operating effectiveness.

We made a judgmental selection of 20 information systems (16 Federal and 4 contractor information systems) from a total population of 78 information systems as of January 21, 2020. Our testing also included DOL-wide information security controls.

METHODOLOGY

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and applicable AICPA standards.[7] Those standards required that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We assessed the effectiveness of the information security program and practices of DOL. Our procedures included the following:

- Inquired of information system owners, system administrators, and other relevant individuals to walk through each control process;
- Inspected the information security practices and policies established by the Office of the Chief Information Officer;
- Inspected the information security practices, policies, and procedures in use across DOL;
- Inspected the artifacts to determine the implementation and operating effectiveness of security controls; and
- Inspected results of vulnerability scanning to determine the implementation of patches, logical access, and baseline compliance.

We performed our fieldwork at DOL's headquarters in Washington, DC, during the period of February 3, 2020, through March 13, 2020. Due to COVID-19, we were required to perform our fieldwork remotely during the period of March 16, 2020, through September 30, 2020. Per our inquiry of DOL management, we were informed DOL did not change the design or operation of security controls and practices as a result of COVID-19. During our performance audit, we met with DOL management to provide a status of the engagement and discuss our preliminary conclusions.

[7] As an Independent Public Accounting firm, KPMG is required to follow standards set forth by AICPA. 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.

CRITERIA

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST SP provide guidelines that are essential to the development and implementation of agencies' security programs. We also utilized DOL's CSH, which outlines DOL's requirements for information security.

APPENDIX B: GLOSSARY

ACRONYM	DEFINITION
AICPA	American Institute of Certified Public Accountants
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CSH	Computer Security Handbook
CSP	Cloud Service Provider
DHS	Department of Homeland Security
DOL	U.S. Department of Labor
DOLCSIRC	DOL Computer Security Incident Response Capability
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PaaS	Platform as a Service
PII	Personally Identifiable Information
PIV	Personal Identity Verification
SaaS	Software as a Service
SECURE	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
SDLC	Software Development Life Cycle
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

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

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

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

Fax
(202) 693-7020

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