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

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2018 FISMA DOL INFORMATION SECURITY REPORT

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: MARCH 13, 2019
REPORT NUMBER: 23-19-001-07-725

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

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

The Department of Labor's (DOL) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct an independent evaluation of DOL's Fiscal Year (FY) 2018 information security programs and practices. OIG monitored KPMG's work to ensure it met professional standards and contractual requirements. KPMG conducted the independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants standards.

KPMG is responsible for the auditors' evaluation and the conclusions expressed in the report. In connection with the contracted work, we reviewed KPMG's report and supporting documentation. This independent evaluation did not constitute an engagement in accordance with *Government Auditing Standards.*

PURPOSE

The objective of this independent evaluation was to determine if DOL implemented an effective information security program for the period October 1, 2017, to September 30, 2018, to include DOL's compliance with Federal Information Security Modernization Act of 2014 (FISMA) and related information security policies, procedures, standards, and guidelines. The determinations were based, in part, on a selection of DOL-wide security controls and a selection of system-specific security controls across 25 information systems and entity-wide controls. Additional details regarding the scope of our independent evaluation are included in Appendix A, *Objective, Scope, and Methodology*.

RESULTS

KPMG reported 36 findings in the following security control areas:

- Risk management
- Configuration management
- Identity and access management

- Data protection and privacy
- Incident response
- Contingency planning

These findings included the following issues:

- Inaccurate system classification
- Unimplemented tools for monitoring software and hardware on the network
- Weaknesses of varying risk levels not mitigated
- Patches not implemented
- Improper separation of duties
- Configuration reviews not performed
- Audit logs not reviewed
- Untimely removal of terminated user accounts
- Incident response technologies undefined
- Contingency failover tests not performed

Consequently, based on results in CyberScope[1], DOL's information security program was not effective for FY 2018.

MOST NOTABLE CONCERN – INFORMATION TECHNOLOGY (IT) GOVERNANCE

Since 2015, OIG has reported issues across multiple systems at DOL resulting from uneven oversight and accountability of the IT control environment by the Chief Information Officer (CIO). In FY 2018, the following findings related to IT Governance were reported:

- Vulnerability scans performed against systems revealed weaknesses, including critical and high, that were not remediated or mitigated in accordance with the DOL's defined timelines. Office of the Chief Information Officer (OCIO) responded it was unable to resolve these weaknesses due to competing priorities. OCIO also acknowledged it could not meet a request to provide 5 weeks of scanning reports, ultimately providing 3 weeks of reports.

- Two agencies had not obtained OCIO approval for risk exemptions with their segregation of duties conflicts.

- OCIO was unable to access an agency's system to monitor audit logs, deferring the responsibility to the agency without verifying it was completed.

- Agency system reclassification occurred without informing OCIO.

[1] Cyberscope is the platform for the FISMA reporting process.

- OCIO lacked tools to authorize what hardware and software could connect to the network.

- OCIO could not provide all requested system baseline configuration and audit logs reviews.

- A lapse in an extended support contract prevented DOL from obtaining patches and updates and left the Department at risk to unpatched vulnerabilities.

The OCIO's lack of oversight of the systems' Information System Security Officers (ISSOs) continues to contribute to the agencies' inability to implement the agency level recommendations and remediate the open prior years' findings, which continue to increase the risk of compromise to confidentiality, integrity, and availability of information within the information systems that support DOL's mission.

We appreciate the cooperation and courtesies OCIO extended us during this audit. OIG personnel who made major contributions to this report are listed in Appendix E.

Elliot P. Lewis
Assistant Inspector General for Audit

FISMA MANAGEMENT SYSTEMS REPORT

KPMG LLP
1676 International Drive
McLean, VA 22102

Elliot Lewis, Assistant Inspector General for Audit
U.S. Department of Labor
200 Constitution Ave., NW
Washington, DC 20210

Re: Fiscal Year 2018 the U.S. Department of Labor's Federal Information Security Modernization Act Management Systems Report

This report presents the results of our independent evaluation 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 Department of Homeland Security (DHS). DHS has prepared the FISMA 2018 questionnaire to collect these responses. FISMA requires that the agency Inspectors General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. DOL contracted with KPMG LLP (KPMG) to conduct this independent evaluation.

We conducted our independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

The objective for this independent evaluation was to determine if DOL implemented an effective FISMA information security program and practices for the period October 1, 2017 to September 30, 2018 for its information systems, including DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We assisted the DOL Office of Inspector General (OIG) in categorizing the identified findings for the CyberScope metrics. We based our work, in part, on a selection of DOL wide security controls and a selection of system-specific security controls across 15 information systems (11 DOL information systems and 4 DOL contractor systems). Additional details regarding the scope of our independent evaluation are included in Appendix A, *Objective, Scope, and Methodology*.

Consistent with applicable FISMA requirements, 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 5 cybersecurity functions[2] and 8 FISMA metric domains[3]. While the security program has been implemented across DOL, we identified 10 findings within 4 of the 5 cybersecurity functions and within 6 of the 8 FISMA metric domains, as follows:

- Identify – Risk Management
- Protect – Configuration Management
- Protect – Identity and Access Management
- Protect – Data Protection and Privacy
- Respond – Incident Response
- Recover – Contingency Planning

In addition, we reported 26 findings to management in 3 out of 5 FISMA metric functions that are relevant to assess DOL's information security management program, as part of our FY 2018 financial statement audit that evaluated controls of 10 DOL financial systems.

We have made recommendations related to these control findings and additional program recommendations to the Chief Information Officer (CIO) that, if effectively addressed by management, should strengthen DOL's information security program.

This independent evaluation did not constitute an engagement in accordance with *Generally Accepted Government Auditing Standards*. KPMG did not render an opinion on DOL's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other information systems not included in our selection is subject to the risks that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

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

KPMG LLP

February 27, 2019

[2] In FY 2018 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*.

[3] As described in the DHS' *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1,* 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 handling, and contingency planning.

BACKGROUND

Federal Information Security Modernization Act

Title III of the E-Government Act of 2002 (the Act), 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. The Act assigns specific responsibilities to agency heads and IGs in complying with requirements of FISMA. The Act is supported by OMB, 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 and magnitude of harm resulting from the 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 operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, we determined through our work, DOL's information security program and practices for its information systems were established and have been maintained for the 5 cybersecurity functions and 8 FISMA metric domains. DOL had consistently implemented its information security program with policies and procedures consistent with NIST standards, but had not implemented metrics to measure and manage implementation of its program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

The FISMA program areas are outlined in the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1* and were prepared by DHS' Office of Cybersecurity and Communications Federal Network Resilience. The CyberScope functions and domains are depicted in Table 1 below.

Table 1: CyberScope Functions and Domains

Cybersecurity Framework Function	**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: FY2018 Inspector General FISMA Reporting Metrics v1.0.1

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 FY 2018 metrics mark a continuation of the work undertaken in FY 2017 to transition the IG evaluation to a maturity model approach. CIGIE implemented maturity models for the FY 2018 FISMA metric domains as follows:

- *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 consistently implement them 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.

While we found weaknesses during our testing, our review found DOL consistently implemented cybersecurity security program policies and procedures that are in line with NIST standards. However, performance metrics have not been established to measure and manage the effectiveness of the program on repeatable and regular near real time frequency.

Furthermore, using the *FY 2018 Inspector General FISMA Reporting Metrics, o*ur evaluation assessed the overall rating of DOL's cybersecurity program and function areas as an overall Level 3, *Consistently Implemented*, which DHS and OMB consider an ineffective level of security.[4]

DHS and OMB have determined that Level 4, *Managed and Measurable,* is considered to be an effective level of security at the domain, function, and overall program level.[5] Ratings throughout the 8 domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions

[4] OMB, DHS, and CIGIE developed the FY 2018 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2018 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*.
[5] Source: FY2018 Inspector General FISMA Reporting Metrics v1.0.1

served as the domain rating. For example, if there are 7 questions in a domain, and the agency received 'defined' ratings for 3 questions and 'managed and measurable' ratings for 4 questions, then the domain rating is 'managed and measurable'. OMB and DHS will ensure that these domain ratings are automatically scored when entered into CyberScope, and IGs and CIOs should note that these scores will rate the agency at the higher level in instances when 2 or more levels are the most frequently rated. Similarly, the same simple majority rule described above was used to calculate the function and overall agency rating.

Table 2 below depicts the DOL OIG's assessed level of security for each functional area.

Table 2: OIG Security Assessment by Functional Area

Cybersecurity Framework Function	OIG Assessment
Identify	Level 3 – Consistently Implemented
Protect	Level 3 – Consistently Implemented
Detect	Level 3 – Consistently Implemented
Respond	Level 3 – Consistently Implemented
Recover	Level 3 – Consistently Implemented

Source: DOL OIG CyberScope entries

During FY 2018, we conducted an evaluation of 15 DOL systems and DOL's entity-wide controls. We identified and reported 10 findings to DOL management in 4 of 5 FISMA metric functions.

In addition, during the audit of DOL's FY18 financial statements, we tested 10 DOL financial systems and identified 26 findings in 3 out of 5 FISMA metric functions that are relevant to DOL's information security management program.

We made recommendations related to our findings that, if effectively addressed by system owners and OCIO management, should strengthen the respective information systems and DOL's information security program. DOL has been implementing corrective actions based on our recommendations and their progress will be evaluated in FY 2019.

We specifically noted the following findings in 4 out of 5 cybersecurity functions, which will be described in detail later in the report:

CYBERSECURITY FUNCTION: IDENTIFY

Domain: Risk Management

- Weakness in the DOL inventory classification
- Weakness in the hardware and software asset inventory process

- Information technology governance and oversight weakness

CYBERSECURITY FUNCTION: PROTECT

Domain: Configuration Management
- Vulnerability assessment weaknesses [6]
- Weaknesses in database and operating server patching processes
- Weakness in entity-wide baseline configuration review process

Domain: Identity and Access Management
- Segregation of duties issues
- User recertification issues
- Weaknesses in entity-wide audit log review process
- Weaknesses in user termination process
- Weaknesses in the DOL remote user session timeout
- Weaknesses in the DOL password settings

Domain: Data Protection and Privacy
- Weakness in the entity-wide incident response reporting capabilities

CYBERSECURITY FUNCTION: RESPOND

Domain: Incident Response
- Weakness in entity-wide incident reporting

CYBERSECURITY FUNCTION: RECOVER

Domain: Contingency Planning
- Weakness in the contingency plan testing process

The *Findings* section of this report presents the detailed findings and the program recommendations for the CIO. The recommendation associated with the specific system findings have been communicated to the system owners.

[6] This finding was identified as part of the FY18 financial statement audit.

FINDINGS

IDENTIFY FUNCTION

The goal of the *Identify* function is to develop the organizational understanding essential to managing cybersecurity risk by identifying and maintaining a hardware and software inventory. By understanding the organization and its mission, the IT resources that support its functions, and related cybersecurity risks, the agency can focus and prioritize its efforts consistent with its risk management strategy and business needs.

We found DOL had policies, procedures, and strategies consistent with NIST standards for managing cybersecurity risk by identifying and maintaining a hardware and software inventory; however, DOL does not utilize continuous monitoring reports/dashboards in managing its program. Additionally, while we reported weaknesses, the majority of the metrics were determined to be at Consistently Implemented (Level 3) for this function, which DHS and OMB consider an ineffective level of security.

RISK MANAGEMENT

Weakness in the DOL Inventory Classification

For 1 of 15 FISMA systems tested, we identified an incorrect system classification within the DOL system inventory. We inspected a system inventory extract from DOL's inventory tool on January 23, 2018, and determined the system was classified as a contractor system. On February 15, 2018, during the FY 2018 DOL FISMA entrance conference with DOL management personnel, we listed the system as a contractor system in the presentation. On May 22, 2018, we sent the audit notification email listing to management as a contractor system. It was not until our meeting with management personnel on May 24, 2018, that we were informed by management that the system was a DOL-owned system. Upon re-inspection of DOL's inventory tool, we noted the classification of the system was changed from a contractor system to a DOL-owned system on May 22, 2018.

OCIO Management stated that they were not aware of the system classification change for the system in the DOL's inventory tool. OCIO management stated that based on the DOL's inventory tool activity log related to the system, the system classification attribute changed from "Contractor System: YES" to "Contractor System: NO" in DOL's inventory tool on May 22, 2018.

The Department of Labor Computer Security Handbook (CSH), Volume 18, edition 5.0, version 1.0, dated December 2017, Program Management Policy, Procedure and Standard, page 6 states:

> DOL's required minimum policies and standards for a system inventory are as follows:
>
> 1. DOL must develop and maintain an inventory of its major information systems in accordance with the policies and standards outlined in the DOL CSH Volume 20. The annual systems inventory shall be included as an appendix in the DOL Security Strategic Program Plan.

Senior 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. By not maintaining an accurate classification of information systems, there is a risk that the needs and requirements pertaining to an information system may be overlooked. Specifically, the monitoring of security controls for the information system may not be occurring because DOL personnel are unaware of who is responsible for specific controls. This can lead to an increased risk in the compromise of integrity, confidentiality, availability of the data contained within the information system.

Weakness in the Hardware and Software Asset Inventory Process

For 1 of 15 FISMA systems tested, we determined that there is no tool in place to determine which hardware and/or software assets can or cannot be introduced into the system if they are not already connected. This could result in unauthorized assets connected to the network without being detected.

DOL management stated that they are currently in the process of configuring a tool to identify, alert, and eventually block unauthorized devices from connecting to the system. OCIO will implement the “identify and alert process” in a phased approach across the National Office and all its sites. OCIO management also stated that the tool is fully deployed on their wireless network and is currently configured to block any rogue devices or unapproved devices. Additionally, another tool is being procured in Quarter 1 of FY19 to address software asset management. Currently, OCIO tracks software via Excel spreadsheets and manages enterprise licenses, which will not allow the software to be installed without the DOL key. Software installations are controlled by those who have permission to do installations, which is typically system administrators, help desk technicians, or users with escalated privileges. All other users are denied.

Volume 5 of the DOL CSH stated DOL's required minimum standards on developing and documenting an information component inventory are as follows:

1. DOL agencies must employ automated mechanisms that, on an on-going basis, detect the presence of unauthorized hardware, software, and firmware components within the information system.

Without a tool in place to block unauthorized devices, it is possible for unauthorized assets to connect to the network undetected. Assets that connect to the network undetected could lead to the loss of the confidentiality, integrity, and availability of communication and services across the enterprise.

Information Technology Governance and Oversight Weakness

DOL management, who is responsible for oversight and accountability for the DOL IT control environment, has not remediated findings in multiple information systems throughout the entity.

Specifically, during FY 2018 testing of DOL's information technology controls, we identified new control findings, in addition to others reported in prior years across DOL systems. Specifically, we found:

- Twelve new findings in the areas of risk management, configuration management, identity and access management, and data protection and privacy; and
- Twenty-four previously reported findings in the areas of identity and access management, incident response, and contingency planning that remain open.

Various findings in the areas of identity and access management, incident response, and contingency planning have continued to exist. New findings in the areas of risk management, configuration management, and data protection and privacy were identified in FY 2018, for which OCIO did not take appropriate action and monitoring of ongoing pervasive deficiencies that have been identified in multiple information systems. Additionally, prior issues continue to exist and new issues have been identified related to management not performing effective testing to determine that issues are closed and where management prematurely closed POA&Ms.

We noted that OCIO and Office of the Assistant Secretary for Administration and Management (OASAM) management, as well as DOL as a whole, have made some improvements in DOL's control environment and have developed plans to implement additional tools and processes in FY 2019 and FY 2020, but not enough progress has been made to remediate prior years' control deficiencies. Furthermore, while system consolidation has lowered the number of findings

identified from prior years, issues remain because of the ongoing implementation of DOL's corrective actions.

Executive Order 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*, dated May 15, 2018, Sec. 4 Emphasizing Chief Information Officer Duties and Responsibilities, states the head of each covered agency shall take all necessary and appropriate action to ensure that:

> (a) consistent with 44 U.S.C. 3506(a)(2), the CIO of the covered agency reports directly to the agency head, such that the CIO has direct access to the agency head regarding all programs that include IT;
> (b) consistent with 40 U.S.C. 11315(b), and to promote the effective, efficient, and secure use of IT to accomplish the agency's mission, the CIO serves as the primary strategic advisor to the agency head concerning the use of IT;
> (c) consistent with 40 U.S.C. 11319(b)(1)(A), the CIO has a significant role, including, as appropriate, as lead advisor, in all annual and multi-year planning, programming, budgeting, and execution decisions, as well as in all management, governance, and oversight processes related to IT; and
> (d) consistent with 40 U.S.C. 11319(b)(2) and other applicable law, the CIO of the covered agency approves the appointment of any component CIO in that agency.

The OCIO's lack of oversight over of the systems' Information System Security Officers (ISSOs) continues to affect the agencies' ability to implement agency level recommendations and close prior year findings. This increases the risk of compromise to confidentiality, integrity, and availability of information within the information systems that support DOL's mission.

PROTECT FUNCTION

The goal of the *Protect* function is to ensure that agencies safeguard their systems, networks, and facilities with appropriate cybersecurity defenses. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the domains of configuration management, identity and access management, data protection and privacy, and security training.

We found DOL had policies, procedures, and strategies consistent with NIST standards for its configuration management program, Identity and Access Management, and Data Protection and Privacy. While we reported weaknesses, the majority of the metrics were determined to be Consistently Implemented (Level 3) for the Protect function, which DHS and OMB consider an ineffective level of security.

CONFIGURATION MANAGEMENT

Vulnerability Assessment Weaknesses

For 3 of 10 financial systems tested during the FY18 financial statement audit, numerous weaknesses were identified during vulnerability and configuration scans that were not remediated or mitigated in accordance with the DOL's defined timelines.

Additionally, we noted baseline security misconfigurations within the financial host tested. We also requested evidence for 5 weekly scanning reports that are sent to the respective agencies for review. However, the agencies were unable to provide evidence of the weekly scanning reports for 2 of the selected weeks.

Security compliance, configuration and patch management processes were not enforced to ensure that vulnerabilities were remediated within established timeframes as agencies resources had competing priorities and lacked sufficient documentation, such as scanning reports.

Volume 17 of the DOL CSH depicts the following minimum required standards regarding flaw remediation:

- DOL information systems must identify, report, and correct information system flaws.
- Relevant security updates (including software and firmware) must be tested for effectiveness and potential side effects on DOL information systems prior to installation in production environments, and then installed on all machines as appropriate except where instances preclude system functionality. In the event that the business functions are not significantly hindered, all updates must be installed in all production, development, and test environments.
- Alerts must be monitored from the vendor, developer, and/or DOL Computer Security Incident Response Capability (DOLCSIRC) regarding flaws in the software.
- Information regarding the patch level of each information system must be tracked by DOL agencies and reported to Office of the Chief Information Officer (OCIO) Security on a monthly basis.
- OCIO Security reserves the right to specify a minimum level of importance (including, but not limited to, minimum requirements) for updates that have been released by approved sources. In instances where OCIO Security does not specify minimum requirements for updates, information system personnel shall develop, implement, and comply with any and all agency

requirements. The minimum requirements for installing updates on information systems are as follows:

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.

- Agencies must monitor for vulnerability and/or patch releases.
- Agencies must review applicable patches when released.

Without consistently enforcing the process for remediating vulnerabilities in the DOL IT environment, there is an increased risk that existing or new vulnerabilities could expose financial information systems and applications to attacks, unauthorized modification, or compromise of data. As security updates are released to mitigate the risk of vulnerabilities affecting operating systems or applications, a lack of timely implementation of these security updates increases the risk of compromise to the confidentiality, integrity, and availability of the data residing on the information system.

Weaknesses in Database and Operating Server Patching Processes

For 3 of 10 systems hosted on the DOL network that were tested for the FY18 financial statement audit, DOL did not consistently follow policies and procedures identified in the CSH for implementing patches that correct security weaknesses.

DOL management stated that due to a lapse in the extended support contract for software, the technical staff was unable to obtain upgrade patch releases by the vendor. DOL management further stated that extended support has since been purchased and they received the latest patches and applied them once they were tested and authorized. KPMG performed testing and validated remediation of the issue.

Additionally, OASAM management stated that patch came out during an OCIO upgrade. The OCIO team made the determination to hold off on installing this patch until all agencies were on the same level to avoid any unforeseen issues that could have potentially delayed the upgrade. OCIO was unable to provide evidence regarding the decision to delay the patch implementation.

Strong configuration management control practices are intended to reduce the risk of system exposure by way of known findings, malicious technical attacks, and unauthorized or unintentional changes. By not appropriately patching the

network to correct security weakness, DOL systems hosted on the network are at risk.

Weakness in Entity-Wide Baseline Configuration Review Process

For 4 of 15 FISMA systems tested, DOL was unable to provide evidence of reviews of baseline configuration scans for selected servers. Further, OCIO was unable to provide any evidence of scan results from 1 server because an agent was not installed.

OCIO management stated that tool is configured with standard configurations from Defense Information Systems Agency (DISA), Center for Internet Security (CIS) and U.S. Government Configuration Baseline (USGCB), but is not fully adhering to all of the OCIO approved baseline requirements for secure configurations. However, OCIO management stated that there is a plan in place to get all operating system baselines into the tool by December 2018. Additionally, OCIO management informed us that the selected server in question has been added to the list of servers for weekly scans going forward. We have not yet validated this statement, but will follow up at a later date.

We determined that the OCIO's configuration baseline compliance tool, is not fully configured with OCIO required baselines and deviations.

Volume 5 of the DOL CSH stated that:

1. Baseline configurations of the information system must be developed, documented, and maintained throughout the system development life cycle.
2. The baseline configuration of the information system must be reviewed and updated at least annually or when a change occurs as an integral part of information system component installations.

Without adhering to DOL security baseline configurations, management cannot ensure that systems are configured restrictively enough to mitigate risks. Failure to comply with DOL policy regarding configuration management causes DOL's systems and information to be vulnerable to damage or loss of confidentiality, availability, and integrity.

Additionally, when configuration scans are not regularly conducted, management cannot ensure that configurations are being maintained according to the required specifications. Failure to identify these potential discrepancies through consistent reviews weakens controls concerning accuracy, confidentiality, and accountability.

IDENTITY AND ACCESS MANAGEMENT

Segregation of Duties (SoD) Issues

For 2 of 10 systems tested during the FY18 financial system audit, we noted that the 2 agencies, had not obtained OCIO approval for risk exemptions with their SoD conflicts. If an agency finds that it cannot implement a DOL CSH policy, procedure, or standard, the agency must obtain a documented risk exemption with approval by the OCIO using the Risk Management Form. Specifically for 1 system, we noted that OCIO had not authorized the risk exemption using the Risk Management Form for SoD issues related to the system and its database administrators. Additionally, an exemption using the Risk Management Form could not be provided for users assigned with conflicting access to the other system's infrastructure layers because 1 was not completed and approved.

OASAM management stated that the delay of approving the risk exemption and issuing the Risk Management Form for a system was due to personnel shifts and organizational realignment. Therefore, additional time was needed to determine which personnel qualified for the risk exemption. We were further informed that a draft was written, but not finalized.

OASAM management also stated that a risk exemption was not needed, and therefore not approved, for a system because the process and access request forms were modified to ensure proper SoD.

Volume 1 of DOL's CSH depicts the Department's minimum required standards on enforcing separation of duties, as follows:

1. Separate duties of general and privileged users as necessary, to prevent malevolent activity without collusion
2. Document separation of duties of individuals
3. Define information system access authorizations to support separation of duties.

Additionally, Volume 12 of DOL's CSH states the following:

> If an agency finds that it cannot implement a DOL CSH policy, procedure or standard, agencies must follow the process outlined in the Enterprise Risk Management Strategy and complete the Risk Management Form....

Failure to periodically review the risks posed by allowing accounts to have privileged access to both the database and the operating system could expose the agency to risks that have not been identified since the last review or that are no longer acceptable to the agency. Specifically, by not enforcing SoD, an

individual with a combination of database administrator access and system administrator access could complete unauthorized transactions, hide unauthorized activity, and/or override controls. Furthermore, without segregating system administrator and database administrator access, an increased risk exists of unauthorized or inadvertent access to data, which compromises the confidentiality and integrity of data. Additionally, if the risk exemption document is not formally reviewed and approved by management, OASAM may not be fully aware of the risks the role conflicts pose and, therefore, would not be able to monitor those risks appropriately.

User Recertification Issues

For 5 of 10 systems tested during the FY18 financial statement audit, we noted that user access to the systems was not appropriately recertified. Specifically, we noted for a system that 2 system administrators were not recertified, a different system had 18 application users with access to migrate source code to production, another system had 12 users with access to develop source code, and 445 employees with active user accounts for a different system were not appropriately recertified in FY18. For a system, 148 user accounts were not part of the recertification process, and 8 accounts were marked to be disabled, but still retained access. There were also 3 system administrator accounts that were not included in the semi-annual recertification for the system.

OASAM, OWCP, ETA and DOL management stated the following reasons for recertification issues:

1. OASAM management stated that due to oversight, a recertification was not appropriately performed for the systems administrators' access rights. OASAM management further stated that an ad hoc recertification is being performed for these users to ensure their access is appropriate.
2. OASAM management stated that due to oversight and the manual nature of the process, a recertification was not completed for all individuals with access to migrate system source code to production.
3. OWCP management stated that 5 of the system user accounts were not initially included in the listing provided to the by OCIO for recertification. For the remaining 7 accounts, OWCP management stated that a development environment account was not needed for these users, and thus was not associated with these users in the recertification listing, as they are not actually developers and do not touch or modify the system source code.
4. DOL management stated that access was not recertified for the 445 individuals because they were unable to obtain responses from the users because the Standard Operating Procedures (SOP) lacked effective security measures that require a response from all users. DOL

management further stated that they intend to add additional layers of security to their Account Recertification SOP to insure a 100 percent response rate.

5. ETA management stated that of the 148 accounts, many were not included in the recertification as the query written for the recertification was done by a previous Analyst (who has since left) and only picked up 'Active' Users and users that have logged in at least once. The users identified as active, but not having a last login date, would not have been included.

Volume 1 of DOL's CSH states the following regarding recertification:

> 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 required based on user need and rights. Annual attestation of this "recertification" is to be provided to OCIO Security.

Failure to periodically review the appropriateness of privileged user access rights or permissions increases the risk of unauthorized access to system's infrastructures, users performing functions that do not match their job descriptions, and potential segregation of duties conflicts will not be detected and prevented timely. These issues also increase the risk of compromise of the confidentiality, integrity, and availability of DOL financial data and other sensitive information. For the administrator accounts not being included in the semi-annual recertification, ETA management stated this was an oversight.

Weaknesses in Entity-Wide Audit Log Review Process

For 4 of 15 FISMA systems tested and 6 of 10 financial systems tested, we noted that system owners did not appropriately review all of their application auditable events. Two of the systems had a Separation of Duties (SoD) Conflict between those reviewing the logs and those who were performing the security functions being logged, whereas the remaining systems did not track and review all the required auditable events.

MSHA, WHD, and ETA management stated the following reasons for the lack of application audit log reviews:

1. MSHA management stated that an infrastructure transfer of a system's audit logs resulted in storage issues, which prevented them from properly monitoring application audit logs during that time.
2. WHD management reported that the untimely submission of monthly application audit logs from WHD's operations and maintenance support

contractor, led to the untimely review of the logs by the WHD Security Team.

3. ETA management stated that reviews of the application audit logs are performed on an as-needed basis. Management performs reviews to conduct trouble shooting of production issues, and semi-annually to trouble shoot the account recertification process. Additionally, ETA management stated the system upgrade project life cycle time caused a resource constraint and did not allow for further enhancements to the project. Once the enhancement is deployed the issue will be closed.

OASAM management stated that DOL System administrators have access to all systems within their environment they can serve as the primary system administrator or as a backup administrator. Currently, OCIO system administrators review the logs associated with their systems and then the Federal Lead performs a subsequent review. OCIO is currently implementing a tool throughout the enterprise at the infrastructure level. The tool will be configured to automate the review of the audit logs and to alert and report on suspicious activity in accordance with the CSH. Until the tool is in place, OCIO will designate primary system administrators for each server. The backup administrator will then be responsible for review of the logs and will rotate between system administrators.

KPMG noted a complicated system architecture contributes to the audit logging issues and because responsibilities are not clearly defined, not all audit logging events required by the CSH were tracked and reviewed

Volume 1 of DOL's CSH states the following:

> Separation of duties addresses the potential for abuse for authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties may include but are not exclusive to the following examples:
>
> a. dividing mission functions and information system support functions among different individuals and/or roles;
> b. conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security);
> c. ensuring Security personnel administering access control functions do not also administer audit functions; and
> d. different administrator accounts exist and are used for different roles.

Volume 3 of DOL's CSH states that the Department requires the following minimum standards on managing information system audit events:

Section 3.1.1:

1. Determine, based on a risk assessment and mission/business needs, that the information system is capable of auditing the following events:
   a. Account creation, modification, disabling, and deletion
   b. Administrative permission executed on user accounts (including but not limited to, inclusion in access groups, reset of passwords, account lockout override)
   c. Administrative permissions executed on a system resource (including but not limited to, addition of users or groups to access lists, creation of sharepoints, creation of new access groups, change of access group permissions)
   d. Failed login attempts and account lock
   e. Use of 'su', 'pu', 'root', and 'administrator', or equivalent accounts
   f. Activity log roll-over, deletion, or editing
   g. All computer-readable data extracts from database containing personally identifiable information (PII)

Section 3.2.1:

1. The information system's audit records are reviewed and analyzed at least monthly for indications of inappropriate or unusual activity and reports findings to designated agency officials.

The ETA CSH, Chapter 403 states:

- Periodic review of the audit logs ensures that the proper information is being captured, security concerns are addressed, problems are mitigated in a timely fashion, and the information will be useful in an investigation. Reviewing audit logs on a regular basis is also necessary to verify that logging is functioning properly and adheres to ETA standards.
- The following events should be audited:
  - Account creation, modification, disabling, and deletion
  - Administrative permissions executed on user accounts (i.e., inclusion in access groups, reset of password, account lockout override)
  - Administrative permissions executed on system resources (i.e., addition of users or groups to access lists, creation of share points, creation of new access groups, change of access group permissions)
  - Execution of privileged functions
  - Failed login attempts and account lockout
  - Use of 'su', 'pu', 'root', 'administrator', or equivalent

- Activity log rollover, deletion, or editing
- All access to PII or data extracts containing PII

The purpose of audit logs is to record user activity that occurred within the information system. Without proper monitoring of all audit log events, incidents may go undetected, increasing the exposure of data contained in the information system. The lack of proper review of audit logs increases the risk that management will not detect inappropriate or unusual activity that may compromise the confidentiality, availability, and integrity of the data residing on the system.

Weaknesses in User Termination Process

For 5 of 10 systems tested during the financial statement audit, we noted that separated employees were not disabled in a timely manner. Specifically, we identified the following:

1. Two user accounts and 1 operating system administrator were disabled more than 10 business days after the user separated from DOL.
2. Twenty-one separated ETA employees retained access to an application account more than 10 days after their separation date.
3. Eight network accounts were not disabled timely after their HR separation date, ranging from 14 to 162 days after the users separation date. We also determined that of those 8 accounts, 2 of the users in question accessed the network after their separation date.
4. Three network accounts were disabled within the 10-day requirement after their HR separation date; however, we noted that each of these 3 accounts accessed the network after their separation date.
5. Four network accounts were not disabled timely after their HR separation date, ranging from 11 to 63 days after the users' separation date. We also determined that, of those, 3 accounts in question accessed the network after their separation date.
6. Twelve separated users for a system were disabled more than 10 days after their HR separation date.
7. OASAM management had not implemented a DOL-wide process to monitor the separation of all contractors that support DOL programs.

Management stated the following reasons for the delay in user termination:

1. Division of Federal Employees Compensation (DFEC) management stated the 2 user accounts that retained access after the associated users' separation are Employees Compensation Appeals Board (ECAB) employees. ECAB is a completely separate entity from OWCP, and

OWCP does not handle their documentation and has no visibility into when they leave DOL. [Auditor Note: Per the DOL CSH, the system owner is ultimately responsible for the security of the system. The operating system administrator account not being removed was an oversight.] Failure to remove the operating system administrator account was an oversight.

2. ETA management stated the user listing provided was from an updated system account management tool released in March 2018. As a result, the listing of users being compared was from 2 different versions of the system and had 2 different versions of how the account management processed worked at the time. As in the previous version of the system, the account management was handled by the system's team with the need for DOL to assist with 90 percent of the work, and the current version of the system is maintained 100 percent by the system's team. Lastly, as some of the accounts were a part of the previous system, which is now decommissioned, the system team was unable to verify any additional information for the accounts noted.

3. For the 4 network accounts, it was the untimely receipt of either notification from the Agency (via ticket or email) to the help desk, as well as the receipt of the proper forms, that caused the failure and was due to their lack of understanding of the requirement. Three of the accounts that were accessed after the separation date was to access their Microsoft Outlook email account before management had removed access to the account and the remaining account was to reactivate the account of a retired individual to update the out of office message.

4. OASAM management stated that network accounts were not being disabled timely because DOL Agencies were not notifying the help desk within the 10 day timeframe outlined in the CSH.

5. DOL management stated the following:
   - For 1 user, the daily separations report showed an HR Process Completion Date 6 days after their HR separation date. No form for the user was submitted before that time. The system's team notified the Project Manager on the same day they received the separations report and coordinate with the agency POC to reassign document ownership. A deactivated form was then submitted and processed.
   - For 2 identified users, there was no daily separation report sent for the day after their separation. Additionally, there was no form submitted.
   - For 2 users, for a few weeks following the users' HR separation date, the daily separations report was blank due to a mistyped configuration value in the HR system that generates the report.

- For 7 users, the daily separations report showed an HR Process Completion Date more than 10 days after the users' HR separation date on the termination listing. For each of those 7 users, their account was deactivated the next day.

Volume 13 of DOL's CSH states that when an employee is terminated, the agency shall:

1. Notify account managers to:
    a. Deactivate the associated accounts within 10 business days from the HR termination effective date (for employees) or COR separation date of record (for contractors) when termination is voluntary; or
    b. Deactivate the associated accounts within 4 hours of such termination (including but not limited to, same day the employee is terminated) if termination is involuntary (including but not limited to, emergency, hostile).

Failure to disable user access upon termination increases the likelihood of unauthorized access to the applications and network, which increases the risk of a compromise of the confidentiality, integrity, and availability of DOL financial data and other sensitive information.

Weaknesses in the DOL Remote User Session Timeout

For 1 of 15 FISMA systems tested, remote user connections were configured to perform session timeouts after 30 minutes of inactivity. We noted that while this setting is in compliance with FISMA metric 31 and FIPS 140-2, the DOL CSH calls for a remote session timeout after 15 minutes of inactivity for any moderate or high information systems.

For 1 of the financial subnetwork systems tested, there were 5 user accounts that had not been logged into for over 100 days, and in some cases up to 1425 days. While DOL policy requires the accounts to be disabled after 60 days, these accounts were not disabled.

OASAM and OCIO management stated that the DOL CSH was not properly updated to reflect the correct remote session timeout setting of 30 minutes, instead of its stated 15 minutes. OASAM and OCIO management stated that the Enterprise Policy and Planning (EPP) team reviewed the CSH and has revised the policy. We verified that Section 3.2.9 of the CSH, Volume 1, was updated to correct the remote session timeout setting.

Regarding the subnetwork user accounts, OASAM management stated that for 1 of the 5 accounts, an error was identified in the tool that missed some accounts, and that a Change Request (CR) was opened to address the bug and upgrade the tool to the latest version. For another account, OASAM management informed us that it was an administrator account that was excluded from the auto-disabled script to allow troubleshooting as required for ETA servers and, after review, the account was found to be in the incorrect Organizational Unit where the auto-disable was not run and the issue was corrected. For the remaining 3 identified accounts, OASAM management stated that the accounts were public and by design, no action is taken on users containing "Public" in their display name, since they are shared email accounts.

Volume 1 of DOL's CSH states that the Department requires the following minimum standards on remote access:

1. Agencies must further assess and correct system configuration upon connection, scan for viruses and malware upon connection, prohibit split tunneling, configure sessions to time-out after 15 minutes of inactivity requiring re-authentication, and audit sessions.
2. DOL's additional required minimum standards on managing information system accounts for Moderate and High information systems are as follows:
    a. The information system must automatically disabled accounts after 60 days of inactivity, and alert the necessary personnel of such an event.

Failure to update the entity-wide policies and procedures can result in inconsistent practices among DOL personnel, which could lead to errors because employees either lack the knowledge of proper procedures or are not held accountable. Additionally, by not enforcing the disabling of inactive accounts within the DOL imposed time requirements, accounts will remain active and prone to compromise for an extended period. These accounts expose the agency to additional risk of unnecessary access to accounts with elevated privileges to system functionality and application data.

Weaknesses in the DOL Password Settings

For 1 of the financial systems tested, the root password for the database server has not changed in accordance with DOL policy. The password for the root account was not changed due to management oversight. OASAM management also stated that the account is accessible to only 4 individuals.

Volume 7 of DOL's CSH states that DOL's required minimum standards on managing information system identification and authentication of Departmental users are as follows:

- Passwords must be changed the first time a user logs on.

- Passwords must be set to automatically expire 90 days or sooner. Password expiration is not to be set to expire on intervals longer than 90 days. In addition, unless authorized by the Information Security Officer (ISO) and/or system owner, passwords cannot be changed in less than 1 day.

Weaknesses in password configuration settings over applications, operating systems, and databases increase the risk of unauthorized access to an environment, and may compromise the confidentiality, integrity, and availability of the data residing on the information system.

DATA PROTECTION AND PRIVACY

Weakness in the Entity-Wide Incident Response Reporting Capabilities

For DOL's entity-wide program tested under FISMA, the Department has not fully identified and defined requirements for incident response technologies regarding data protection and privacy security tools that are integrated with intrusion detection and prevention systems.

OCIO Management stated that they are reconsidering technologies to support the incident response process for intrusion detection and intrusion prevention. This initiative would include defining all information technology network egress components within the DOL infrastructure to implement adequate technology for use in responding to incidents.

Volume 8 of the DOL CSH states that:

> The agency employs automated mechanisms to support the incident handling process.

Without implementation of appropriate incident response tools, or defining requirements for certain incident response technologies, DOL is susceptible to cyber security attacks of incidents which could lead to a compromise in the confidentiality, integrity, and availability of data utilized by individuals with access to, or reliance upon, DOL systems or processes.

RESPOND FUNCTION

The *Respond* function ensures that agencies have policies and procedures in place that detail how they will respond to cybersecurity events, with a focus on incident response testing and communications.

We found DOL had policies, procedures, and strategies consistent with NIST standards for incident response. While we reported weaknesses, the majority of the metrics were determined to be Consistently Implemented (Level 3) for this function, which DHS and OMB consider an ineffective level of security.

INCIDENT RESPONSE

Weakness in Entity-Wide Incident Reporting

For the DOL entity-wide program tested under FISMA, incidents from OASAM, WHD, OFCCP, and ETA were not reported to the DOL Computer Security Incident Response Capability (DOLCSIRC) team within 1 hour. Additionally, for 1 of 10 systems tested during the financial statement audit, 1 of 5 cyber incidents selected for testing were not reported from the DOLCSIRC team to the US-CERT within 1 hour. Further, DOL has not fully identified and defined requirements for incident response technologies regarding intrusion detection and prevention systems.

OASAM and OCIO Management stated that DOLCSIRC does not have control over the sub agencies or their users reporting incidents to DOLCSIRC, nor are the incidents official until received by DOLCSIRC. OASAM management also stated that the incidents were not reported timely to US-CERT due to the time needed for the agencies to analyze and then provide the information to DOLCSIRC. Additionally, OCIO is reconsidering technologies to support the incident response process for intrusion detection and intrusion prevention. This initiative would include defining all information technology network egress components within the DOL infrastructure to implement adequate technology for use in responding to incidents.

Volume 8 of the DOL CSH states that the Department's required minimum standards on incident reporting are as follows:

1. All computer security incidents involving a DOL Information System with a confirmed impact to confidentiality, integrity or availability must be reported to DOLCSIRC within 1 hour of being positively identified by the agency. DOLCSIRC will report to US-CERT within 1 hour incidents impacting confidentiality, integrity or availability to DOL systems or information. If an

incident is received after business hours it will be processed the next business day. DOLCSIRC will make the final determination if an event is an incident and will report to US-CERT within ONE HOUR of the final determination.

2. All non-cyber related incidents should be reported to DOLCSIRC within 1 hour of a confirmed breach. Non-cyber is defined as items such as digital cameras, tokens (only if used after loss), paper, voice, and media (USB thumb drive, CD, etc.). If an incident is received after business hours it will be processed the next business day.

3. All PII incidents are to be reported within 1 hour of discovery regardless if suspected or confirmed. If an incident is received after business hours it will be processed the next business day.

4. Suspected incidents are to be reported to DOLCSIRC within 1 business day. If an incident is received after business hours it will be reported the next business day. These incidents are not required to meet the 1 hour time frame, but should be on the same day of discovery.

Incident response capabilities are vital in ensuring that the DOLCSIRC is able to report all incidents to the US-CERT timely. Failure to report an incident to DOLCSIRC or US-CERT in a timely manner could result in the actions to detect and protect against malicious code or other critical DOL information and systems being delayed, allowing those systems and information to be compromised.

RECOVER FUNCTION

The *Recover* function supports timely recovery to normal operations to reduce the impact from a cybersecurity event by focusing on contingency planning.

We found DOL had policies, procedures, and strategies consistent with NIST standards for contingency planning. While we reported weaknesses, the majority of the metrics were determined to be Consistently Implemented (Level 3) for this function, which DHS and OMB consider an ineffective level of security.

CONTINGENCY PLANNING

Weakness in the Contingency Plan Testing Process

For 4 of 15 FISMA systems tested, failover and failback contingency testing was not performed. The network provides the overall support system for non-

applicant support such as back-ups. A lack of coordination among agencies ISSOs and OASAM (the hosting organization for contingency planning activities resulted in failover and failback testing not being performed.

OASAM and OCIO Management informed us that failover/failback contingency testing is only required periodically. The DOL CSH does not define the time period for when it should be tested; it only provides an example. Therefore, it is left to each agencies' discretion when to conduct contingency plan testing. Management stated that each agency needs to coordinate any testing required with OCIO as each contingency plan test may have a different time for their test. Further, OCIO has documented test cases where failover has occurred for infrastructure as well as a Disaster Recovery site for core services to support the infrastructure.

Volume 6 of the DOL CSH states the following policy, procedures, and standards must be implemented for all Low, Moderate, and High information systems:

1. DOL agencies perform tests of the contingency plan for the information system to determine the effectiveness of the plan, and the organizational readiness to execute the plan, reviews the contingency plan test results, and initiates corrective actions, if needed.
2. A full failover test to a hot/warm/cold site must be performed periodically (e.g. annually or bi-annually) if the site is identified as a part of the contingency plan.
3. The contingency plan 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.

DOL's additional required minimum standard on developing a contingency plan for Moderate and High risk information systems is as follows*:*

1. The contingency plan development must be coordinated with agency elements responsible for related plans (including but not limited to, Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Cyber Incident Response Plan, Crisis Communications Plan, Critical Infrastructure Plan, Insider Threat Implementation Plan, and Occupant Emergency Plan).

Without performing information system failover tests in a timely manner, DOL has an increased risk that data residing within the information system may not be restored in the event of data corruption or loss.

CONCLUSION

While we found weaknesses during our testing, our review found DOL had consistently implemented cybersecurity security program policies and procedures that are consistent with NIST standards. Furthermore, using the *FY 2018 Inspector General FISMA Reporting Metrics,* our evaluation assessed the overall rating of DOL's cybersecurity program and function areas as an overall Level 3, *Consistently Implemented*, which DHS and OMB consider an ineffective level of security.[7]

DOL management, responsible for oversight and accountability for the DOL IT control environment, has not remediated the widespread findings in multiple information systems throughout the entity, some of which were first identified by the OIG in 2003. This lack of management oversight and accountability for the DOL IT control environment has resulted in ongoing, unnecessary risk to the confidentiality, integrity, and availability of DOL's information.

To be consistent with FISMA, DOL should strengthen its information security risk management framework; enhance IT oversight and governance to address these weaknesses; and adhere to its information security policies, procedures and controls.

[7] The scoring methodology is described in the DHS' *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1, May 24, 2018* which requires a Managed and Measurable rating (Level 4) to be considered effective as determined by the entries in CyberScope.

RECOMMENDATIONS

Although DOL had established an information security program and practices across the organization, we identified numerous findings that may limit the Department's ability to adequately protect the organization's sensitive information and information systems. Specifically, management charged with oversight and accountability for the DOL information security program has not taken appropriate action to address these deficiencies, many of which have been reported by the OIG in prior reports.

Without appropriate security, DOL cannot adequately protect its mission assets. As such, agency systems and the sensitive data they contain are at risk. The deficiencies we identified could negatively affect the confidentiality, integrity, and availability of agency systems and PII. To be consistent with FISMA, the CIO should provide the resources and oversight to address these weaknesses and ensure DOL agencies and systems adhere to its information security policies, procedures and controls.

We recommend the Chief Information Officer:

1. Conduct a risk assessment to identify the root causes of the identified deficiencies;
2. Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies that have been communicated to DOL management;
3. 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;
4. Monitor the agencies' ongoing progress to ensure that established procedures and controls are operating effectively; and
5. Develop and implement performance metrics that will be used to manage and measure the effectiveness of the DOL information security program.

APPENDIX A: OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

Did DOL implement effective FISMA minimum information security requirements?

In fulfilling the objective above, we performed an evaluation of DOL's information systems to evaluate the effectiveness of the information security program and the implementation of controls which includes policies, procedures, and practices to determine whether the Department meets OMB and FISMA required IT security controls. The NIST 800-53 Rev. 4 publication defines security control effectiveness as the extent to which the 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 also, performed additional testing of security control areas as required by DHS, OMB, CIGIE, and other oversight organizations.

SCOPE

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1,* dated May 24, 2018. We reviewed DOL information security program for a program-level perspective and then examined how each of the information systems selected for our testing selection implemented these policies and procedures for operating effectiveness.

We made a selection of 15 information systems (11 DOL and 4 DOL contractor information systems) from a total population of 63 major applications and general support systems (GSS) as of February 12, 2018. Our testing also include DOL-wide information security controls. Additionally, we evaluated controls of 10 DOL financial systems as part of the financial statement audit.

METHODOLOGY

To assess the effectiveness of the information security program and practices of DOL, our scope 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 OCIO.
- 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.

We performed our fieldwork at DOL's headquarters offices in Washington, District of Columbia (D.C.) during the period of February 15, 2018, through September 30, 2018. During our evaluation, we met with DOL management to provide a status of the engagement and discuss our preliminary conclusions.

We conducted our independent evaluation in accordance with the CIGIE's Quality Standards for Inspection and Evaluation and applicable AICPA standards. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

Criteria

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the FY 2018 FISMA evaluation:

NIST, FIPS and/or Special Publications[8]

- FIPS Publication 199*, Standards for Security Categorization of Federal Information and Information Systems*

[8] Per OMB FISMA reporting instructions, while agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800 series) in how agencies apply the guidance. However, NIST FIPS are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

- CFO Council Enterprise Risk Management (ERM) Playbook
- SANS Top 20 Critical Security Controls for Effective Cyber Defense
- Cloud Computing Contract Best Practices
- Cybersecurity Strategy and Implementation Plan
- Federal Acquisition Regulation; FAR Case 2007-004, *Common Security Configurations*
- Federal Continuity Directive 1
- Federal Cybersecurity Workforce Assessment Act of 2015
- Federal Enterprise Architecture (FEA) Framework
- FedRAMP Standard Contract Clauses
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- FY 2018 Chief Information Officer FISMA Metrics
- FY 2018 Senior Agency Official for Privacy FISMA Metrics
- Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors*
- National Archives and Records Administration (NARA) Guidance on Information Systems Security Records
- National Insider Threat Policy
- National Cybersecurity Workforce Framework Volume 1.0
- NIST Supplemental Guidance on Ongoing Authorization
- NIST Special Publication 800-128; *Guide for Security-Focused Configuration Management of Information Systems*
- NIST Special Publication 800-122, *Guide for Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST Special Publication 800-184, *Guide for Cybersecurity Event Recovery*
- NIST Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management*
- NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*
- NIST Special Publication 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*
- NIST Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*
- NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*

- NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- NIST Special Publication 800-60 Revision 1, Volume *I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-63-2, *Electronic Authentication Guideline*
- NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organization*
- NIST Cybersecurity Framework (CSF)
- NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- Federal Enterprise Architecture (FEA) Framework, Volume 2
- NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- SANS Institute Center for Internet Security Critical Security Controls
- United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines
- Presidential Policy Directive, *United States Cyber Incident Coordination*

OMB Policy Directives

- OMB Circular A-130, *Managing Information as a Strategic Resource*
- M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum 04-25*, Reporting Instructions for the Federal Information Security Management Act*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- *OMB Memorandum M-08-05, Implementation of Trusted Internet Connections*
- *OMB Memorandum M-17-09, Management of Federal High Value Assets*
- *OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information*
- *OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- *OMB Memorandum M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*

United States Department of Homeland Security

- Department of Homeland Security (DHS) Cyber Incident Reporting Unified Message

DOL Policy Directives

- DOL Computer Security Handbook Edition 5.0, Version 1.0 dated December 2017

APPENDIX B: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

SUBJECT: Management Response to the DRAFT REPORT – FY 2018 FISMA DOL Information Security, Report Number: 23-19-001-07-725

This memorandum addresses the above-referenced DRAFT REPORT – *FY 2018 FISMA DOL Information Security* issued to the DOL Chief Information Officer (CIO) on January 7, 2019, for management's review and response.

DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve security for our information systems and data. Further, we appreciate that the report notes that "DOL has consistently implemented its information security program with policies and procedures consistent with NIST standards".

The security of DOL's information and information systems is one of the Department's top priorities, and we remain committed to ensuring the Department implements safeguards to protect its information and information systems, and understands the importance of adequately managing identified security risks. Through risk-based decision making and strategic planning, OCIO continues to strengthen its cybersecurity program by implementing corrective actions; resulting in considerable progress to address or significantly lower risks associated with each of the areas referenced in the independent auditor's report.

Management responses to the specific control area deficiencies noted in the report, and to the resulting recommendations, are detailed below. Documentation and other artifacts related to the corrective actions taken by OASAM/OCIO are available upon request from the OIG.

IT GOVERNANCE CONCERN

While management acknowledges the individual findings attributed in the report to IT Governance, we do not concur that the findings result "from uneven oversight and accountability of the IT control environment by OASAM/OCIO." The CIO has the necessary authority to direct IT activities within the Department of Labor.

Management has taken action regarding each of the findings.

Finding	Status

Vulnerability Scans	OCIO has taken steps to ensure vulnerability scanning occurs on at least a weekly basis for all systems, and that reports are sent to appropriate stakeholders for review and action.
Risk Exemption Approval	OCIO has adjudicated these risk exemption requests. In addition, to prevent reoccurrence OCIO has taken actions to enhance the risk exemption process; to include timely adjudication of exemption requests, and review of approved exemptions.
Audit Log Monitoring	Prior to the audit, OCIO had obtained tools to help with audit log collection and review, and deployment of these tools continue to help address this finding. In addition, OCIO will provide policies, procedures, training, and support to ensure audit logs are monitored by the appropriate parties.
System Reclassification	The system classification has been corrected and validated. Also, in response, OCIO has updated governing procedures and templates, and performs bi-annual reviews of system inventory for accuracy and completeness.
Authorized HW/SW	Prior to the audit, OCIO had obtained tools to authorize and control hardware and software usage. Deployment of these tools continue to address this finding.
Baseline Configurations and Audit Log Reviews	OCIO has taken steps to ensure configuration baselines are standardized, and the configuration management processes are aligned with the DOL's CSH requirements.
Lapse in Support Contract Prevented Patches	Once this condition was discovered, the extended support was promptly purchased and patches were obtained and applied. OASAM has consistently provided OCIO with the requested resources for cybersecurity.

In addition, the Department is currently undertaking a Shared Services initiative that includes all DOL IT services being consolidated under the OCIO. This initiative will further bolster the CIO's existing authority and oversight in areas such as vulnerability scanning, risk management, system monitoring, and classification.

CYBERSECURITY FUNCTION: IDENTIFY

Management does not concur with the *IT Governance and Oversight Weakness* identified by the evaluators, as OCIO has sufficient authority to implement Department-wide IT governance and oversight.

Management concurs with the other findings regarding this cybersecurity function and has taken the following corrective actions to address:

- Revised Major Information Systems (MIS) inventory reporting template to include a field for entering ownership status.

- The Computer Security Handbook (CSH) inventory methodology has been updated to reflect details of responsibilities and process for both the annual inventory procedure as well as out-of-cycle inventory changes.
- Continue to work with agencies to verify their asset inventory and management process. Ensured bi-annual review for accuracy and completeness.
- Implemented a solution to address Software Asset Management.
- Continue configuring a solution to identify, alert, and eventually block unauthorized devices from connecting to the network.

CYBERSECURITY FUNCTION: PROTECT

Management concurs with the findings regarding this cybersecurity function and has taken the following corrective actions to address:

- Strengthened DOL's information security continuous monitoring (ISCM) program with the deployment of additional security monitoring tools and features to automate and prioritize the deployment of critical security software patches and system configuration settings.
- Enhanced DOL's efforts to prioritize and remediate vulnerabilities and ensure applications are up-to-date to support the latest platform; implemented a weekly patch and vulnerability remediation reporting process.
- Enhanced DOL's efforts to prioritize the configuration management processes to ensure configuration baselines are standardized, and the configuration management processes are aligned with the DOL's CSH requirements.
- Reinforced Enterprise Risk Management to enhance the risk exemption process; to include timely adjudication of exemption requests, and review of approved exemptions.
- Completed implementation of acquired Identity and access management (IAM) tools; moving from the Development to Production phase of the enterprise solution. This implementation affords the Department the capability of integrating DOL applications, leading to the centralization of Access Control functions and reduction of operational risk for managing accounts. DOL expects to implement additional IAM capabilities in FY19.
- Implemented a security information and event management (SIEM) for the purpose of automating the review of audit logs.
- Implemented auto-generated lists of separated employees and contractors, sent regularly to agency Information Security Officers (ISOs) for review. The auto-generated lists and reviews will increase timely disabling of accounts for separated users.
- Revised DOL CSH to reflect remote session timeout setting requirements to align with mission needs.
- Obtained and are implementing new detection capabilities (Web Application Firewall, Intrusion Detection system, and File Integrity) to monitor for and mitigate malware.

CYBERSECURITY FUNCTION: RESPOND

Management concurs with the findings regarding this cybersecurity function and has taken the following corrective actions to address:

- Developed and implemented incident reporting and response policies and supporting standard operating procedures.
- Continued to capture incident reporting in a database that is maintained by the DOL Computer Security Incident Response Capability (CSIRC) team members and is used to track incidents.
- Continued use of Department of Homeland Security-contracted (DHS) tools to detect and prevent intrusion attempts.
- Continue to enhance the functionality of the SIEM tool to alert incident response personnel when issues are identified.

CYBERSECURITY FUNCTION: RECOVER

Management concurs with the findings regarding this cybersecurity function and has taken the following corrective actions to address:

- Ensured contingency plans were developed and implemented for DOL information systems.
- Ensured contingency plans are reviewed and tested on an annual basis. Annual testing of contingency plans includes testing of the backup process and functional exercises to include the testing of alternate sites, where applicable.

During the course of FY 2019, DOL will continue to implement processes to ensure agencies adhere to information security policies, procedures and controls. The enhancement of oversight and enterprise cybersecurity capabilities continues to be a top priority to DOL.

RECOMMENDATIONS

Management concurs with the recommendations in the report and intends to take the following actions to address.

OCIO will:

- Conduct a risk assessment to identify and document the root causes of the identified deficiencies;
- Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies in this report;
- Direct efforts 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;

- Monitor ongoing progress to ensure that established procedures and controls are operating effectively; and
- Develop and implement performance metrics that will be used to manage and measure the effectiveness of the DOL information security program.

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

cc: Bryan Slater, Assistant Secretary for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Geoffrey Kenyon, Principal Deputy Chief Financial Officer
Paul Blahusch, Chief Information Security Officer (CISO) (Acting)
Scott Davis, Deputy Chief Information Security Officer (CISO) D/CISO
Muhammad Butt, Branch Chief, Enterprise Policy and Planning (EPP)

APPENDIX C: AUDITOR'S REBUTTAL

We have reviewed management's response to our report and found the CIO concurs with the findings, with the exception of the IT Governance finding. The CIO is responsible for the control environment, including the people, processes, and technology used to implement and monitor the controls established by the OCIO. As we noted in our report, we identified 12 new findings in the areas of risk management, configuration management, identity and access management, and data protection and privacy. Further, our report references the 24 previously reported findings in the areas of identity and access management, incident response, and contingency planning that remain open. We have also noted the Department's progress in developing corrective action plans to address the open recommendations. However, during the performance of our FY 2018 evaluation, these corrective action plans were still in process or management did not fully address the root cause to enable acceptance of the corrective action plans. In FY 2019, we will evaluate the status of the Department's development and implementation of corrective action plans.

APPENDIX D: GLOSSARY

ACRONYM	DEFINITION
Act, The	Title III of the E-Government Act of 2002
AICPA	American Institute of Certified Public Accountants
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
CP	Contingency Planning
CSH	Computer Security Handbook
D.C.	District of Columbia
DHS	Department of Homeland Security
DOL	U.S. Department of Labor
DOLCSIRC	DOL Computer Security Incident Response Capability
EW	Entity Wide
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GSS	General Support System
IA	Identity and Access Management
ISCM	Information Security Continuous Monitoring
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Planning
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
KPMG	KPMG LLP
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer

ACRONYM	DEFINITION
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
PII	Personally Identifiable Information
POC	Point of Contact
RA	Risk Assessment
RHEL	Red Hat Enterprise Linux Operating System
RM	Risk Management
SANS	SysAdmin, Audit, Network and Security [Institute]
SOD	Separation of Duties
SOP	Standard Operating Procedure
ST	Security Training (ST)
US-CERT	United States Computer Emergency Readiness Team

APPENDIX E: ACKNOWLEDGEMENTS

The audit team included:

Christian Arsenault, Auditor
Brian Devaney, Audit Manager
Stephen Fowler, Audit Director
LeslieAntoinett Hunter, Program Analyst

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

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

Email
hotline@oig.dol.gov

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

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Room S-5506
Washington, DC 20210