U.S. Department of Labor

Office of Inspector General—Office of Audit

**REPORT TO THE CHIEF INFORMATION OFFICER**

# FY 2019 FISMA DOL INFORMATION SECURITY REPORT: IMPLEMENTATION OF SECURITY TOOLS HINDERED BY INSUFFICIENT PLANNING

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

Elliot P. Lewis
Assistant Inspector General for Audit

**DATE ISSUED: December 23, 2019**
**REPORT NUMBER: 23-20-002-07-725**

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

# BRIEFLY…

## FY 2019 FISMA DOL INFORMATION SECURITY REPORT: IMPLEMENTATION OF SECURITY TOOLS HINDERED BY INSUFFICIENT PLANNING

**December 23, 2019**

## WHY OIG PERFORMED THE EVALUATION

DOL spends approximately $730 million annually on its Information technology (IT) assets that support the programs needed to fulfill DOL's mission. As IT plays an integral role in providing the services and operations needed to fulfill DOL's mission, it is imperative that DOL maintain a strong IT security program to protect these assets. Ineffective IT security programs increase the risk of unavailable service, security breaches and unreliable information. Under the Federal Information Security Modernization Act of 2014 (FISMA), Inspectors General are required to perform annual independent evaluations of their agency's IT security program and practices.

## WHAT OIG DID

We contracted with KPMG LLP to conduct an independent evaluation of the DOL Fiscal Year (FY) 2019 information security programs, for the period October 1, 2018, to September 30, 2019. KPMG partly based its determinations on tests of a selection of DOL's entity-wide security controls and system-specific security controls across 20 DOL information systems.

## READ THE FULL REPORT

http://www.oig.dol.gov/public/reports/oa/2019/23-20-002-07-725.pdf

## WHAT THE EVALUATION FOUND

KPMG reported findings for all FISMA cybersecurity functions, and 6 of 8 FISMA metric domains into Department of Homeland Security's FISMA reporting system, which determined DOL's information security program was not effective for FY 2019.

DOL's Office of Chief Information Officer (OCIO) was unable to provide timelines and plans for any of the information security tools that were not fully implemented, indicating the utilization of these tools was not properly managed. For ten of the FISMA metrics, OCIO did not meet a higher score because it had not fully implemented the necessary tools. In these ten metrics, the score for FY 2019 was the same as it had been in FY 2018, indicating a lack of progress in implementing a tool to address the issue at hand. The ten metrics where OCIO had not fully implemented the necessary tools covered areas including Risk Management, Configuration Management, and Identity and Access Controls.

We believe the OCIO should strive for accurate self-assessments of its information security progress. Where the OCIO had accurate self-awareness of the condition of its information security program, such as in the area of Security Training, KPMG identified positive progress in improving DOL's position. Security Training was responsible for 6 of the 21 upward trending ratings in FY 2019. Conversely, in the area of Risk Management, where the OCIO had the lowest accuracy rate of self-awareness, KPMG found non-concurrence in 8 of the 12 questions. The better the accuracy of OCIO's self-assessment, the more effective OCIO will be at addressing unresolved issues in other domain areas.

Based on these issues, we remain concerned about the continued improvements needed in the OCIO's oversight and accountability over the Department's IT control environment.

## WHAT OIG RECOMMENDED

We made twenty recommendations to improve information security and establish performance metrics. The CIO concurred with most of these recommendations.

**U.S. Department of Labor**

Office of Inspector General
Washington, D.C. 20210

## INSPECTOR GENERAL'S REPORT

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

The Department of Labor's (DOL) Office of Inspector General (OIG) contracted with KPMG LLP to conduct an independent evaluation of DOL's Fiscal Year (FY) 2019 information security programs. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal Inspectors General, or an independent external auditor, to conduct annual evaluations of the information security programs and practices of their respective agencies.

OIG monitored KPMG's work to ensure it met professional standards and contractual requirements. KPMG's independent evaluation was conducted 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 was responsible for the auditors' evaluation and the conclusions expressed in the report, while 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, 2018, to September 30, 2019. The determinations were based, in part, on the testing of a selection of DOL's entity-wide security controls and system-specific security controls across 20 of its information systems. Additional details regarding the scope of the independent evaluation are included in Appendix A, *Objective, Scope, and Methodology*, of KPMG's attached report.

## RESULTS

KPMG reported findings for all FISMA cybersecurity functions, and 6 of 8 FISMA metric domains, which included the following issues:

- Annual assessment of third party cloud services not performed
- 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
- Reportable incidents were not reported timely to US-CERT
- Contingency failover tests not performed

After entering the results of KPMG's testing into the Department of Homeland Security's CyberScope system, CyberScope determined DOL's information security program was not effective for FY 2019.

## NOTABLE CONCERNS

OCIO was unable to provide timelines and plans for any of the information security tools not fully implemented; indicating utilization of these tools was not properly managed. For ten of the FISMA metrics, OCIO did not meet a higher score because it had not fully implemented the necessary tools. In these ten metrics, the score for FY 2019 was the same as it had been in FY 2018, indicating a lack of progress. The ten metrics where OCIO had not fully implemented the necessary tools covered areas including Risk Management, Configuration Management and Identity and Access Controls.

Additionally, we believe the OCIO should strive for accurate self-assessments of its information security progress. Where the OCIO had accurate self-awareness of the condition of its information security program, such as in the area of Security Training, KPMG identified positive progress in improving DOL's position. Security Training was responsible for 6 of the 21 upward trending ratings in FY 2019. Conversely, in the area of Risk Management, where the OCIO had the lowest accuracy rate of self-awareness, KPMG found non-concurrence in 8 of the 12 questions. The better the accuracy of OCIO's self-assessment, the more effective OCIO will be at addressing unresolved issues in other domain areas.

Based on these issues, we remain concerned about the uneven oversight and accountability of the IT control environment by the OCIO.

In responding to the Draft Report, the CIO agreed with most of the OIG's recommendations but took issue with several points made in the report (see Management Response for the entirety of the CIO response). Of particular note, the CIO disagreed with our concern regarding accurate self–assessments, stating that the OCIO intentionally overstated its responses to the self-assessment in an effort to ensure KPMG would perform additional work to identify where the information security program measured up to a managed and measurable risk level, and where it fell short. In several meetings with the CIO and OCIO management held early in the audit process, the self-assessment and testing processes were discussed. During those meetings, KPMG clearly conveyed that the self-assessment should be an accurate representation of the current state of the Department's IT Security posture. Further, KPMG stated that the OIG would also be evaluating what was required for the Department to meet Level 4 (an effective score) for all questions, regardless of the self-assessment outcome, to help the Department determine what was required to meet that Level.

The CIO also stated in the response that after OCIO's completion of the self-assessment, an additional detailed evaluation guide was provided. The document the CIO referred to is part of the Department of Homeland Security's (DHS) annual FISMA guidance for the CIO, IG and Senior Agency Official for Privacy, and was available on the DHS public website. The IG metrics, evaluation guide and the DHS website were provided to OCIO management during the initial meetings and again during the review.

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

Elliot P. Lewis

Elliot P. Lewis
Assistant Inspector General for Audit

# Fiscal Year 2019 Independent Evaluation of the U.S. Department of Labor’s Federal Information Security Modernization Act of 2014 Management Systems Report

December 19, 2019

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

# Table of Contents

KPMG LLP
Suite 900
8350 Broad Street
McLean, VA 22102

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

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

This report presents the results of our independent evaluation of the 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, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2019 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor to perform the independent evaluation as determined by the IG. DOL Office of Inspector General (OIG) contracted KPMG LLP (KPMG) to conduct this independent evaluation and monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent evaluation in accordance with 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 assess the effectiveness of DOL's information security program and practices, including DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines for the period October 1, 2018 to September 30, 2019. We based our work on a selection of DOL-wide security controls and a selection of system-specific security controls across 15 selected DOL information systems and 5

DOL contractor information systems.[1] Additional details regarding the scope of our independent evaluation are included in Appendix A, Objective, Scope, and Methodology. Appendix B contains a glossary of terms used in this report.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, DOL established and maintained its information security program and practices for its information systems for the five cybersecurity functions[2] and eight FISMA metric domains.[3] Based on the results entered into CyberScope, we determined that DOL's overall information security program was ineffective[4] because a majority of the FY 2019 FISMA metrics were rated Consistently Implemented (Level 3). We reported deficiencies impacting specific CyberScope questions in Identify (risk management), Protect (configuration management, identity and access management, and data protection and privacy), Detect (information security continuous monitoring [ISCM]), Respond (incident response), and Recover (contingency planning).

In our report, we have provided the Chief Information Officer (CIO) 7 findings[5] and 20 recommendations that when addressed should strengthen DOL's information security program. The DOL CIO generally agreed with our findings and recommendations (see Management Response, page 21).

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

[2] OMB, DHS, and CIGIE developed the FY 2019 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2019, the eight IG FISMA metric domains were aligned with the five cybersecurity functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[3] As described in DHS's *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.3, April 9, 2019,* the eight FISMA metric domains are risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

[4] The scoring methodology that is described in DHS's *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.3, April 9, 2019,* requires a Managed and Measurable rating (Level 4) to be considered effective as computed by the entries in CyberScope. Ratings throughout the eight FISMA domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the function and domain rating.

[5] The 7 findings incorporate 23 system-level and entity-wide findings that we issued during our testing.

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 DOL information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Sincerely,

KPMG LLP

December 19, 2019

# BACKGROUND

## Agency Overview

DOL's mission is to foster, promote, and develop the welfare of the wage earners, job seekers, and retirees of the United States; improve working conditions; advance opportunities for profitable employment; and assure work-related benefits and rights. That mission includes administering and enforcing more than 180 federal laws. These mandates and the regulations that implement them cover many workplace activities for about 10 million employers and 125 million workers.

## Federal Information Security Modernization Act

Title III of the E-Government Act of 2002 (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, the agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk 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.

# OVERALL EVALUATION RESULTS

The FISMA program areas are outlined in the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.3,* and were prepared by DHS's Office of Cybersecurity and Communications Federal Network Resilience. The CyberScope functions and domains are listed in Table 1 below.

Table 1: CyberScope Functions and Domains

| 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: FY 2019 Inspector General FISMA Reporting Metrics v1.3

The five specific CyberScope functions are described in detail below:

- *Identify.* Develop organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities by identifying and maintaining a hardware and software inventory.
- *Protect*. Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.
- *Detect*. Develop and implement appropriate activities to identify a cybersecurity event.
- *Respond*. Develop and implement appropriate activities to take action regarding a detected cybersecurity event.
- *Recover.* Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity event.

The maturity model definitions for the FY 2019 FISMA metric domains are:

- *Level 1 (Ad Hoc)*. An agency lacks a formalized program and performs activities in a reactive manner.
- *Level 2 (Defined)*. An agency has a formalized program with comprehensive policies, procedures, and strategies consistent with NIST standards but fails to 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.

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, DOL established and maintained its information security program and practices for its information systems for the five cybersecurity functions and eight FISMA metric domains. Based on the results entered into CyberScope, we determined that DOL's overall information security program was ineffective because a majority of the FY 2019 FISMA metrics were rated Consistently Implemented (Level 3). We reported deficiencies impacting specific CyberScope questions in Identify, Protect, Detect, Respond, and Recover.

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

Table 2: IG FISMA Metric Maturity Level by Functional Area

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

Source: IG CyberScope entries

Table 3 depicts the FY18 to FY19 year-over-year improvement to or degradation in the IG metric ratings for each of the cybersecurity domains:

Table 3: DOL OIG FISMA Metric Ratings Trend, by Domain - FY19 Compared to FY18

| Cybersecurity Domain | FY 19 to FY18: IG Metric Questions Trending Up | FY 19 to FY 18: Metric Questions Trending Down | FY 19 to FY18: IG Metric Questions No Change |
|---|---|---|---|
| Risk Management | 2 | 2 | 8 |
| Configuration Management | 2 | 0 | 6 |
| Identity and Access Management | 5 | 0 | 4 |
| Data Protection and Privacy | 2 | 0 | 3 |
| Security Training | 6 | 0 | 0 |
| ISCM | 0 | 0 | 5 |
| Incident Response | 2 | 1 | 4 |
| Contingency Planning | 2 | 0 | 5 |
| TOTAL | 21 | 3 | 35 |

Source: IG CyberScope entries for FY 2018 and FY 2019

Table 4 compares the number of metric questions in each domain and whether we either agreed to, or disagreed with, DOL management's self-assessment for fiscal year 2019. In no instance was the rating higher than management's self-assessment rating.

Table 4: IG Rating Compared to Management's Self-Assessment Rating

| Domain | IG Rating Does not Concur with Management's Self-Assessment | IG Rating Concurs with Management's Self-Assessment |
|---|---|---|
| Risk Management | 8 | 4 |
| Configuration Management | 6 | 2 |
| Identity and Access Management | 4 | 5 |
| Data Protection and Privacy | 3 | 2 |

| Domain | IG Rating Does not Concur with Management's Self-Assessment | IG Rating Concurs with Management's Self-Assessment |
|---|---|---|
| Security Training | 0 | 6 |
| ISCM | 4 | 1 |
| Incident Response | 6 | 1 |
| Contingency Planning | 5 | 2 |
| TOTAL | 36 | 23 |

Source: KPMG analysis of DOL's self-assessment and IG CyberScope entries for FY 2019[6]

During FY 2019, we conducted an evaluation of 20 DOL systems and DOL's entity-wide controls, and we identified and reported 23 findings to the system and entity-wide control owners. The findings were identified in all of the FISMA metric functions and in 6 out 8 of the FISMA metric domains.

DOL has been implementing various tools from the DHS continuous diagnostic monitoring (CDM) program, which will assist in the overall management of the information security program and allow DOL to enhance their monitoring of controls.

[6] There are 59 FY2019 IG FISMA metric questions that require an IG response.

# FINDINGS

Over the past year, DOL has made strides in implementing tools from the CDM program that, once operational, will provide insights, metrics, and reports/dashboards to senior management and assist them with risk-based decisions. However, for these tools to provide the necessary information to senior management, DOL also needs to develop and implement performance metrics to measure the performance of the cybersecurity functions. We requested project plans for the implementation of the tools referenced by DOL management; however, management failed to provide approved project plans that document the planned completion dates of these implementation projects.

The *Fiscal Year (FY) 2019 Inspector General Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 1.3*, dated April 9, 2019, states the following:

> Level 4, Managed and Measurable, is considered to be an effective level of security at the domain, function, and overall program level by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the function and domain rating.

We determined DOL's information security program to be ineffective based on the entries in CyberScope where a majority of the FY 2019 FISMA reporting metrics were rated Consistently Implemented (Level 3).

## FINDING 1. IDENTIFY – RISK MANAGEMENT

The objective of the *Identify* function in the cybersecurity risk framework is to manage cybersecurity risk to the systems, people, assets, data, and capabilities of DOL. When an agency understands the cybersecurity risk that threatens their mission and services, they are able to establish controls and processes to manage and prioritize risk management decisions.

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets commensurate with their risk environment. Risk management is the process of identifying, assessing, and controlling threats to an organization's operating environment. These threats, or risks, could stem from a wide variety of sources, including budget uncertainty, natural disasters, and cybersecurity threats. A sound risk management plan and program that has been developed to address the various risks that can impact an agency's mission will allow the agency to establish an information security program based on these documented risk management decisions.

During our evaluation procedures, we determined that certain areas of DOL's risk management program had implemented policies and procedures for conducting annual inventory of information systems, conducting hardware and software inventories, conducting supply chain risk management, and third-party monitoring. However, we determined DOL did not establish performance metrics and monitoring processes to effectively manage and measure its risk management program. In addition, there were instances where program management did not retain or document their review of oversight of third parties or have tools in place to prevent or disable unauthorized assets or software from connecting to DOL networks.

NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, states that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. To accomplish this, risk management must be addressed at the enterprise, mission, business process, and information system levels. Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions), (ii) assess risk, (iii) respond to risk once determined, and (iv) monitor risk on an ongoing basis using effective organizational communication and a feedback loop for continuous improvement in the risk-related activities. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision-making is integrated into every aspect of the organization.

Management did not prioritize implementation of risk management metrics and performance monitoring to effectively manage and measure its risk management program, nor did they implement the tools they identified to support risk management tasks. Management also did not monitor that programs were maintaining appropriate documentation in order to demonstrate effective operation for several risk management control areas.

Failure to appropriately define performance metrics for risk management and failure to maintain appropriate documentation of the successful functionality of risk management controls could result in instances where significant IT risk factors for the department's IT program are not considered when making risk-based decisions for security. IT risks may lead to insufficient controls in place to reduce risk or monitor those risks sufficiently, resulting in potential unauthorized access or unauthorized changes to IT systems. These situations could have an impact on the availability, confidentiality, or integrity of DOL data.

## FINDING 2. PROTECT – CONFIGURATION MANAGEMENT

The objective of the *Protect* function in the cybersecurity framework is to develop and implement appropriate safeguards to ensure the delivery of critical services of DOL. The protect function supports the ability of DOL to limit, contain, or prevent the impact of a cybersecurity event. This function is accomplished by proper configuration management, identity and access management, data protection and privacy, and security training processes.

FISMA requires agencies to develop an information security program that includes policies and procedures to ensure compliance with minimally acceptable system configuration requirements. Configuration management refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations. DOL indicated that they are in the process of overhauling their change management process by implementing a new software tool that will provide additional insights and be able to produce metrics and reports for management.

During our evaluation procedures, we determined DOL failed to implement performance metrics to monitor the effectiveness of the configuration management program of DOL systems. We identified several change management deficiencies such as:

a) Lack of a control to monitor for hot fixes and service packs for operating systems and databases supporting DOL servers not associated with a Common Vulnerability Exposure (CVE) that lead to a number of required patches not applied to production systems;
b) Critical and high vulnerabilities that were not remediated in a timely manner, which could have potentially left DOL production systems exposed to known vulnerabilities;
c) Weaknesses with DOL's process to document the monitoring of configuration management baselines for 8 of 15 systems we tested that we assess as impacting the organization's ability to consistently implement the information security architecture; and
d) Configuration management policies and procedures that were not updated to reflect the current control responsibility for reviewing and updating baseline configurations.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, recommends integrating information security into configuration management processes. Security-focused configuration management of information systems involves a set of activities that can be organized into four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring. A key component of security-focused configuration management is monitoring, which involves validating that information systems are adhering to organizational policies, procedures, and approved secure configuration baselines. When inconsistencies are identified, the organization should take action to mitigate resulting security risks. Monitoring processes are also needed to identify software security updates and patches that need to be installed for an organization's technology environment. Unpatched or outdated software can expose an organization to increased risk of a cyberattack.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors and that the organization is to establish an organization-defined benchmark for taking corrective actions to remediate flaws identified.

In addition, NIST SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies* states that for products and systems, including mobile devices, applying patches corrects security and functionality problems in software and firmware and reduces opportunities for exploitation.

Management did not prioritize implementing change management performance metrics and did not prioritize monitoring of system owners' compliance for updating production systems to the latest patch or vulnerability levels. Management also did not prioritize documenting the periodic review of system baseline configurations or establishing a process to monitor for patches that are not associated with CVEs. Additionally, management did not prioritize updating the configuration management policy and procedures to define control responsibilities over reviewing and updating baseline configurations.

Failure to define change management metrics, failure to keep production systems on the most up-to-date patch levels, failure to remediate known vulnerabilities in a timely manner, and failure to document the periodic review of system baselines all could result instances of unauthorized changes being introduced to DOL production systems. Unauthorized changes could have a potential impact on the confidentiality, availability, or integrity of DOL data.

## FINDING 3. PROTECT – IDENTITY AND ACCESS MANAGEMENT

Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as 'need to know.' The supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges. These activities are collectively referred to as the identity, credential and access management (ICAM). DOL is currently in the process of implementing tools that will assist with single sign-on, user management, and controlling privileged access. DOL has implemented strong authentication methods for user access, including onboarding service accounts, in their privileged access tool. DOL has also implemented Federal Information Processing Standards (FIPS) compliant remote access solutions for all users. We also determined that DOL needs to finalize the implementation of these tools that will enhance the identity access and management controls and institute performance metrics so they are able manage and measure the identity and access management program at DOL.

During our evaluation procedures, we determined DOL management failed to implement ICAM performance metrics to manage and measure the ICAM control area. We further determined that at the system level, many DOL systems are still not consistently performing access recertifications, reviewing audit logs, maintaining user access authorizations, or configuring session termination settings.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* states that information system audit records should be reviewed and analyzed for inappropriate or unusual activity. Further, NIST SP 800-53 states the organization should specify authorized users of the information system, including their group and role membership, and account privileges and the need for accounts are to be reviewed for compliance periodically. Additionally, NIST SP 800-53 specifies an information system should automatically terminate a user session after a specified period of inactivity.

Management did not prioritize implementing identity and access management-related performance metrics, compliance monitoring of system owners performing user recertification, audit log reviews of privileged users, or compliance with access configuration settings.

Without documented performance metrics, DOL is unable to track performance of controls and determine if they are operating effectively. Failure to monitor whether system owners are periodically recertifying access, configuring inactivity settings, and periodically reviewing audit logs may lead to instances of unauthorized access not being detected timely and could potentially impact the availability, confidentiality, or integrity of DOL data.

## FINDING 4. PROTECT – DATA PROTECTION AND PRIVACY

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and disclosure necessary to protect personal privacy and proprietary information. In today's digital world, effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource* requires federal agencies to develop, implement, and maintain agency-wide privacy programs that, where PII is involved, play a key role in information security and proper implementation of the NIST Risk Management Framework. Although the head of each federal agency remains ultimately responsible for ensuring that privacy interests are protected and for managing PII responsibly within their respective agency, Executive Order 13719, *Establishment of the Federal Privacy Council* requires agency heads to designate a senior agency official for privacy who has agency-wide responsibility and accountability for the agency's privacy program.

During our evaluation procedures, we identified PII breaches that were not reported timely to the United States Computer Emergency Readiness Team (US-CERT). In addition, we also identified instances where database settings were not enabled to encrypt data at rest that contained PII information. Management informed us that they have mitigating controls in place such as encrypting data in transit and when data is transferred to a mobile device; however, this does not address the requirement of encrypting sensitive data at rest.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that an organization should report security incidents to the organization's incident response capability within an organization-defined period of time. NIST SP 800-53, Revision 4 also states that an organization should have its information systems configured to protect the confidentiality and integrity of data at rest.

DOL management did not prioritize reporting incidents, including PII incidents, to US-CERT and DOL Computer Security Incident Response Capability (DOLCSIRC) in a timely manner. DOL management also did not prioritize encrypting sensitive data at rest as required for FIPS-199 moderate-rated information systems.

Failure to report PII security incidents to appropriate incident reporting capabilities in a timely manner could expose DOL to unnecessary reputational risks. When sensitive data at rest is not encrypted, a user with unauthorized access could obtain this information, which could potentially impact the confidentiality, availability, or integrity of DOL data.

## FINDING 5. DETECT – INFORMATION SECURITY CONTINUOUS MONITORING

The objective of the *Detect* function in the cybersecurity framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The cybersecurity framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation and to maintain knowledge of threats and security control effectiveness.

To further enhance the government's ISCM capabilities, Congress established the CDM program. The CDM program provides agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

During our evaluation procedures, we determined the DOL ISCM strategy policy that documents ISCM performance metrics has not been updated since 2014. The current version contains information on planned activities from 2014 to 2016 for the implementation of tools and operations, but does not provide details as to how these tools and operations are used for the current ISCM program.

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Best practices for implementing ISCM are outlined in NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. SP 800-137 notes that a key component of an effective ISCM program is a comprehensive ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

NIST SP 800-137 emphasizes that an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies, and as part of a broader risk management strategy. Once a strategy is defined, NIST SP 800-137 notes that the next step in establishing an effective ISCM program is to establish and collect security-related metrics to support risk-based decision-making throughout the organization. An ISCM strategy is periodically reviewed and updated to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, that metrics remain relevant, and that data are current and complete.

Management did not prioritize updating the ISCM strategy documentation. DOL management indicated that the DOL ISCM strategy is integrated throughout all risk management activities and incorporated into strategy and planning documents such as the enterprise risk management strategy, DOL System Development Lifecycle Management Manual, FedRAMP (Federal Risk and Authorization Management Program) Continuous Monitoring Strategy Guide, Enterprise Security Operations Center CM (configuration management) Process, DOLGSS (general support system), Security CM, and the agency Annual Security Assessment report.

Failure to keep ISCM policies and procedures up to date with current ISCM metrics could leave significant risks to DOL's IT program undetected. These undetected risk factors may leave DOL systems vulnerable to external and internal threats that could result in unauthorized access or unauthorized changes that could potentially impact the confidentiality, availability, or integrity of DOL data.

## FINDING 6. RESPOND – INCIDENT RESPONSE

The objective of the *Respond* function in the cybersecurity framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes policies and procedures for incident response.

During our evaluation procedures, we determined that DOLCSIRC failed to report several DOL reportable incidents in a timely manner to US-CERT due to management oversight and failure to follow established incident reporting procedures.

NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide* notes that an incident response process consists of four main phases: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. It further notes that establishing an incident response capability should include creating an incident response policy and plan; developing procedures for performing incident handling and reporting; and establishing relationships and lines of communications between the incident response team and other groups, both internal and external to the agency.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* states that an organization should report security incidents to the organization's incident response capability within an organization-defined period of time.

Incident reporting control owners failed to follow proper procedures due to management oversight, and they failed to report the incidents in a timely manner to US-CERT.

Failure to report security incidents to appropriate incident reporting capabilities in a timely manner could expose DOL information systems to threats and instances of unauthorized access. Unauthorized access could result in unauthorized changes to production DOL systems that could potentially impact the availability, confidentiality, or integrity of DOL data.

## FINDING 7. RECOVER – CONTINGENCY PLANNING

The objective of the *Recover* function in the cybersecurity framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The cybersecurity framework outlines contingency planning processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event.

During our evaluation procedures, we determined DOL management had not appropriately implemented contingency planning performance metrics in order to achieve a managed and measurable contingency planning program. In addition, we determined that data backup functionality using the department's backup software tool was not functioning appropriately for a period during the evaluation because of a technical configuration error.

FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization. Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, provides best practices for information system contingency planning. It highlights the importance of conducting a business impact analysis, which helps identify and prioritize information systems and components critical to supporting the organization’s mission and business processes, as a foundational step to effective contingency planning. A business impact analysis allows an organization to measure priorities and interdependencies (internal or external to the entity) by risk factors that could affect mission-essential functions.

An additional important factor for information system contingency planning, noted in NIST SP 800-53, is its integration with other function areas. NIST SP 800-53 highlights the importance of closely coordinating contingency planning with incident-handling activities so that organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. For information system contingency planning, it is important to put in place procedures to use the results of contingency testing as part of an enterprise risk management program to make risk-based decisions at an enterprise level.

Management did not prioritize appropriately documenting contingency planning metrics. Management did not have appropriately documented compensating data backup controls and mechanisms in place to mitigate the impact of the technical configuration error that caused the interruption to the data backup tool.

Failure to appropriately design contingency planning metrics and failure to appropriately back up DOL data may result in instances where backup and recovery operations are not completely identified and ready to operate in case of a disaster. Inoperable or improperly designed contingency planning procedures and tools may lead to system outages that could potentially impact the availability of DOL data.

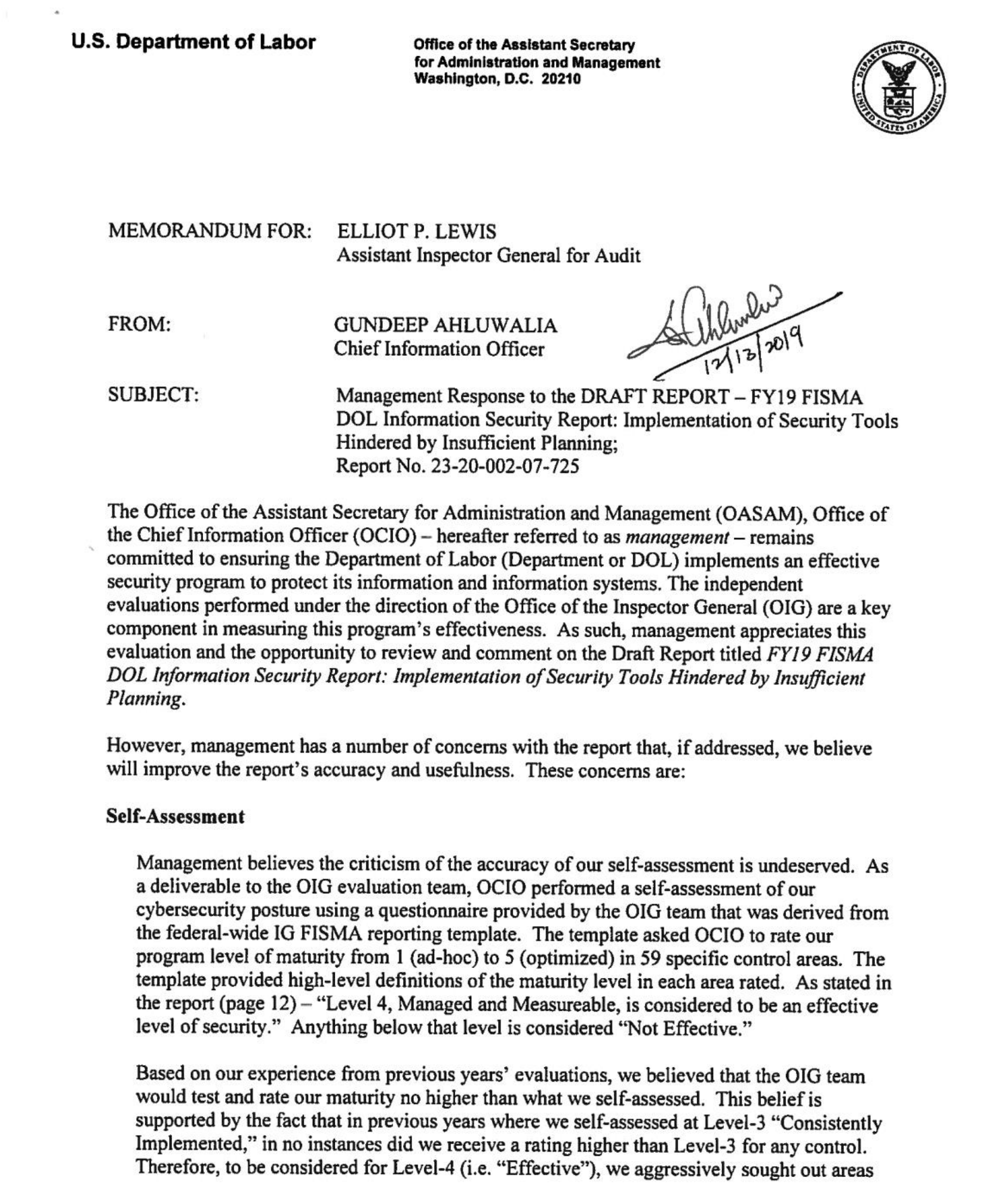
# RECOMMENDATIONS

We recommend the CIO:

1. Perform a reconciliation of the current state of each DOL information system and the related classification to the information documented for each system in Cyber Security Assessment and Management and reconcile any differences.
2. Implement technologies for both DOL and the Bureau of Labor Statistics to detect and prevent unauthorized hardware and software from connecting to the local DOL network.
3. Verify that annual assessments of third-party providers, including cloud service providers, are formally documented, reviewed, and signed by appropriate levels of management.
4. Implement SECURE Technology Act requirements to address organizational cyber supply chain risk.
5. Develop and implement performance metrics for configuration management.
6. Design and implement controls and policies to formally perform and document the periodic review of baseline configuration scans across DOL servers and databases.
7. Design and implement controls to monitor DOL assets for missing patches, service packs, hot fixes, and other software updates that are not associated with a CVE.
8. Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner.
9. Finalize the implementation of the new software tool for configuration management.
10. Review and update configuration management policies and procedures to define pertinent change management responsibilities and control boundaries.
11. Finalize the implementation of the access control technologies.
12. Develop and implement access control performance metrics.
13. Design and implement controls to perform and document a periodic review of audit logs that report privileged user activity.
14. Periodically conduct PII training to enforce PII incident reporting guidelines for timely reporting of PII incidents and enforce the PII incident reporting control process for PII incidents.
15. Implement data encryption configurations/solutions at the server level for data at rest for sensitive information (PII).
16. Update the ISCM strategy guide with current ISCM performance metrics.
17. Periodically conduct training to review the incident management standard operating procedure and incident response reporting guidelines with all agencies so they are aware of procedures prior to incident occurrence.

18. Enforce the incident response monitoring process and procedures to verify that incidents are reported to DOLCSIRC and US-CERT in a timely manner in accordance with DOL policy.
19. Develop and implement contingency planning performance metrics.
20. Enhance backup monitoring controls to reduce backup failures and increase responsiveness to backup failures.

# MANAGEMENT'S RESPONSE TO THE REPORT



**U.S. Department of Labor**

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

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

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

12/13/2019

SUBJECT: Management Response to the DRAFT REPORT – FY19 FISMA DOL Information Security Report: Implementation of Security Tools Hindered by Insufficient Planning;
Report No. 23-20-002-07-725

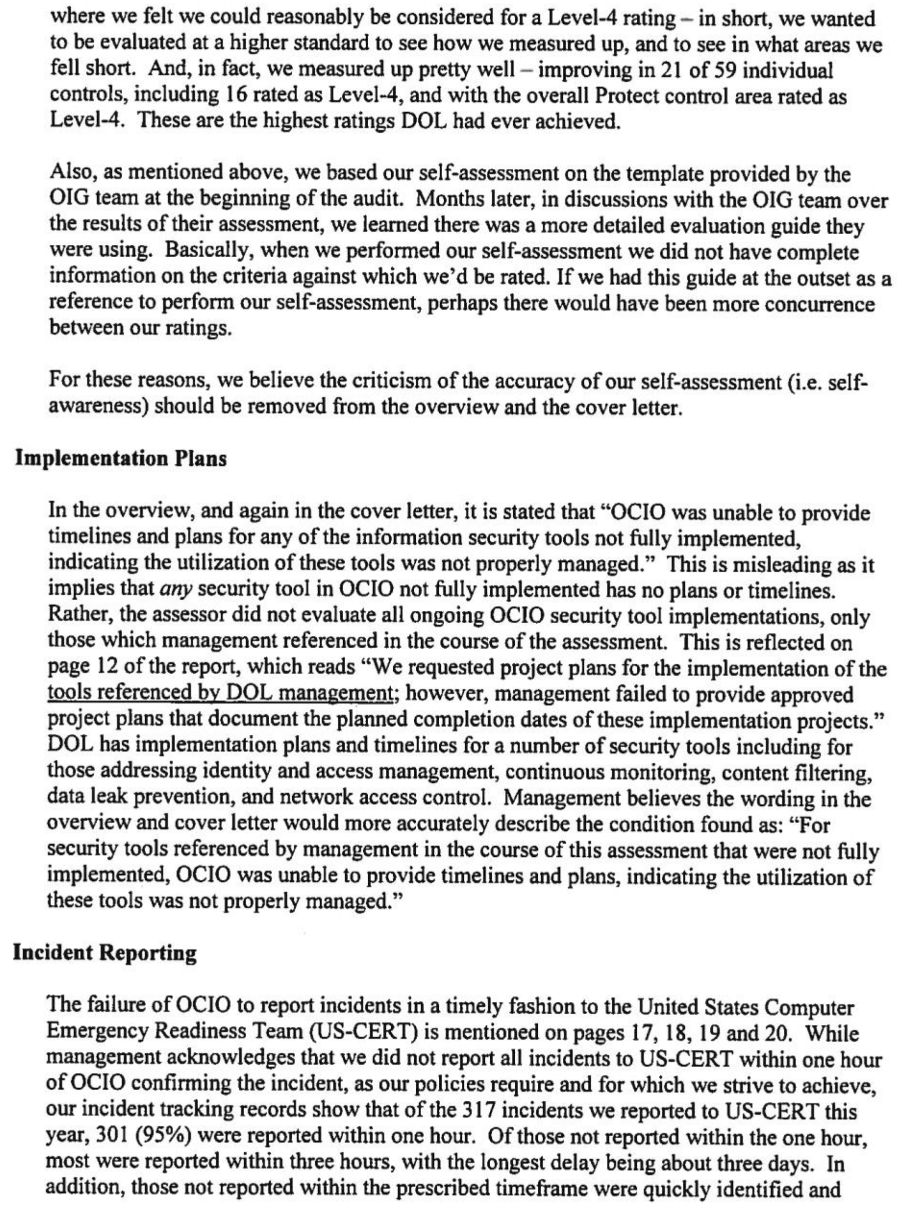
The Office of the Assistant Secretary for Administration and Management (OASAM), Office of the Chief Information Officer (OCIO) – hereafter referred to as *management* – remains committed to ensuring the Department of Labor (Department or DOL) implements an effective security program to protect its information and information systems. The independent evaluations performed under the direction of the Office of the Inspector General (OIG) are a key component in measuring this program's effectiveness. As such, management appreciates this evaluation and the opportunity to review and comment on the Draft Report titled *FY19 FISMA DOL Information Security Report: Implementation of Security Tools Hindered by Insufficient Planning*.

However, management has a number of concerns with the report that, if addressed, we believe will improve the report's accuracy and usefulness. These concerns are:

**Self-Assessment**

Management believes the criticism of the accuracy of our self-assessment is undeserved. As a deliverable to the OIG evaluation team, OCIO performed a self-assessment of our cybersecurity posture using a questionnaire provided by the OIG team that was derived from the federal-wide IG FISMA reporting template. The template asked OCIO to rate our program level of maturity from 1 (ad-hoc) to 5 (optimized) in 59 specific control areas. The template provided high-level definitions of the maturity level in each area rated. As stated in the report (page 12) – "Level 4, Managed and Measureable, is considered to be an effective level of security." Anything below that level is considered "Not Effective."

Based on our experience from previous years' evaluations, we believed that the OIG team would test and rate our maturity no higher than what we self-assessed. This belief is supported by the fact that in previous years where we self-assessed at Level-3 "Consistently Implemented," in no instances did we receive a rating higher than Level-3 for any control. Therefore, to be considered for Level-4 (i.e. "Effective"), we aggressively sought out areas



where we felt we could reasonably be considered for a Level-4 rating – in short, we wanted to be evaluated at a higher standard to see how we measured up, and to see in what areas we fell short. And, in fact, we measured up pretty well – improving in 21 of 59 individual controls, including 16 rated as Level-4, and with the overall Protect control area rated as Level-4. These are the highest ratings DOL had ever achieved.

Also, as mentioned above, we based our self-assessment on the template provided by the OIG team at the beginning of the audit. Months later, in discussions with the OIG team over the results of their assessment, we learned there was a more detailed evaluation guide they were using. Basically, when we performed our self-assessment we did not have complete information on the criteria against which we'd be rated. If we had this guide at the outset as a reference to perform our self-assessment, perhaps there would have been more concurrence between our ratings.

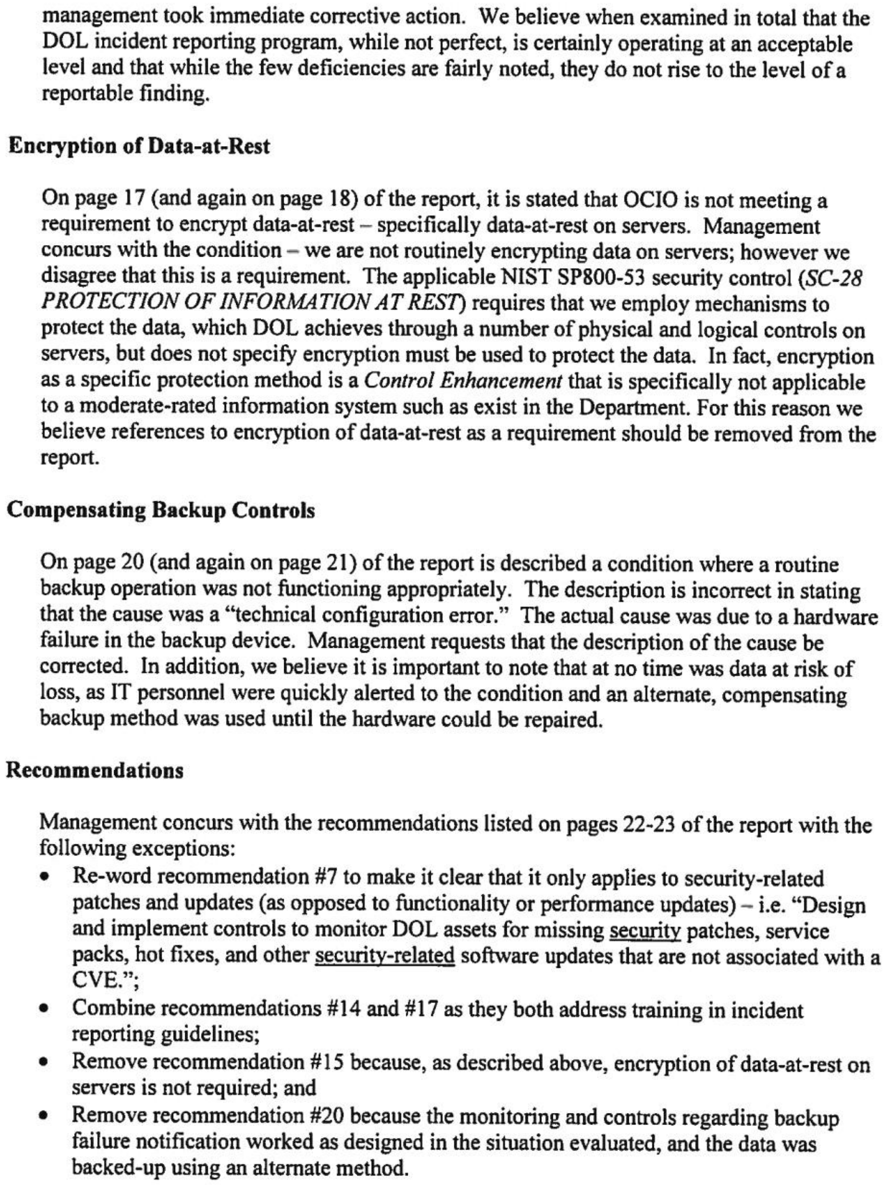
For these reasons, we believe the criticism of the accuracy of our self-assessment (i.e. self-awareness) should be removed from the overview and the cover letter.

**Implementation Plans**

In the overview, and again in the cover letter, it is stated that "OCIO was unable to provide timelines and plans for any of the information security tools not fully implemented, indicating the utilization of these tools was not properly managed." This is misleading as it implies that *any* security tool in OCIO not fully implemented has no plans or timelines. Rather, the assessor did not evaluate all ongoing OCIO security tool implementations, only those which management referenced in the course of the assessment. This is reflected on page 12 of the report, which reads "We requested project plans for the implementation of the tools referenced by DOL management; however, management failed to provide approved project plans that document the planned completion dates of these implementation projects." DOL has implementation plans and timelines for a number of security tools including for those addressing identity and access management, continuous monitoring, content filtering, data leak prevention, and network access control. Management believes the wording in the overview and cover letter would more accurately describe the condition found as: "For security tools referenced by management in the course of this assessment that were not fully implemented, OCIO was unable to provide timelines and plans, indicating the utilization of these tools was not properly managed."

**Incident Reporting**

The failure of OCIO to report incidents in a timely fashion to the United States Computer Emergency Readiness Team (US-CERT) is mentioned on pages 17, 18, 19 and 20. While management acknowledges that we did not report all incidents to US-CERT within one hour of OCIO confirming the incident, as our policies require and for which we strive to achieve, our incident tracking records show that of the 317 incidents we reported to US-CERT this year, 301 (95%) were reported within one hour. Of those not reported within the one hour, most were reported within three hours, with the longest delay being about three days. In addition, those not reported within the prescribed timeframe were quickly identified and



management took immediate corrective action. We believe when examined in total that the DOL incident reporting program, while not perfect, is certainly operating at an acceptable level and that while the few deficiencies are fairly noted, they do not rise to the level of a reportable finding.

**Encryption of Data-at-Rest**

On page 17 (and again on page 18) of the report, it is stated that OCIO is not meeting a requirement to encrypt data-at-rest – specifically data-at-rest on servers. Management concurs with the condition – we are not routinely encrypting data on servers; however we disagree that this is a requirement. The applicable NIST SP800-53 security control (*SC-28 PROTECTION OF INFORMATION AT REST*) requires that we employ mechanisms to protect the data, which DOL achieves through a number of physical and logical controls on servers, but does not specify encryption must be used to protect the data. In fact, encryption as a specific protection method is a *Control Enhancement* that is specifically not applicable to a moderate-rated information system such as exist in the Department. For this reason we believe references to encryption of data-at-rest as a requirement should be removed from the report.

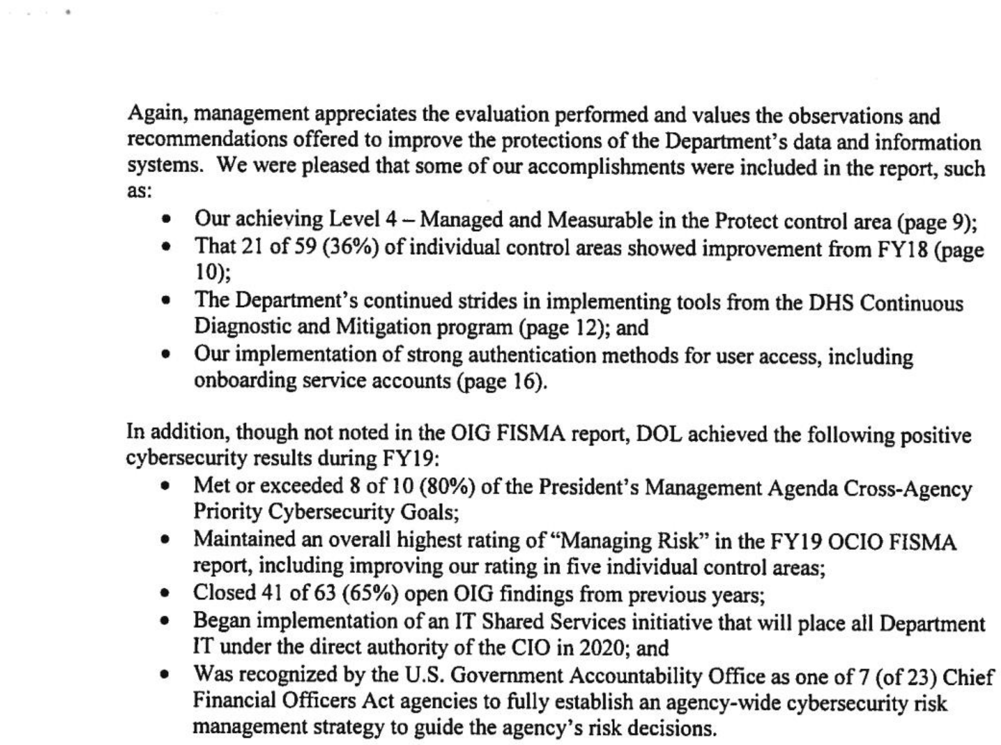
**Compensating Backup Controls**

On page 20 (and again on page 21) of the report is described a condition where a routine backup operation was not functioning appropriately. The description is incorrect in stating that the cause was a "technical configuration error." The actual cause was due to a hardware failure in the backup device. Management requests that the description of the cause be corrected. In addition, we believe it is important to note that at no time was data at risk of loss, as IT personnel were quickly alerted to the condition and an alternate, compensating backup method was used until the hardware could be repaired.

**Recommendations**

Management concurs with the recommendations listed on pages 22-23 of the report with the following exceptions:

- Re-word recommendation #7 to make it clear that it only applies to security-related patches and updates (as opposed to functionality or performance updates) – i.e. "Design and implement controls to monitor DOL assets for missing security patches, service packs, hot fixes, and other security-related software updates that are not associated with a CVE.";
- Combine recommendations #14 and #17 as they both address training in incident reporting guidelines;
- Remove recommendation #15 because, as described above, encryption of data-at-rest on servers is not required; and
- Remove recommendation #20 because the monitoring and controls regarding backup failure notification worked as designed in the situation evaluated, and the data was backed-up using an alternate method.



Again, management appreciates the evaluation performed and values the observations and recommendations offered to improve the protections of the Department's data and information systems. We were pleased that some of our accomplishments were included in the report, such as:

- Our achieving Level 4 – Managed and Measurable in the Protect control area (page 9);
- That 21 of 59 (36%) of individual control areas showed improvement from FY18 (page 10);
- The Department's continued strides in implementing tools from the DHS Continuous Diagnostic and Mitigation program (page 12); and
- Our implementation of strong authentication methods for user access, including onboarding service accounts (page 16).

In addition, though not noted in the OIG FISMA report, DOL achieved the following positive cybersecurity results during FY19:

- Met or exceeded 8 of 10 (80%) of the President's Management Agenda Cross-Agency Priority Cybersecurity Goals;
- Maintained an overall highest rating of "Managing Risk" in the FY19 OCIO FISMA report, including improving our rating in five individual control areas;
- Closed 41 of 63 (65%) open OIG findings from previous years;
- Began implementation of an IT Shared Services initiative that will place all Department IT under the direct authority of the CIO in 2020; and
- Was recognized by the U.S. Government Accountability Office as one of 7 (of 23) Chief Financial Officers Act agencies to fully establish an agency-wide cybersecurity risk management strategy to guide the agency's risk decisions.

# 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 that include policies, procedures, and practices to determine whether the Department meets OMB- and FISMA-required IT security controls. The NIST SP 800-53 Rev. 4 publication defines security control effectiveness as the extent that controls are (1) implemented correctly, (2) operating as intended, and (3) producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies. We also, performed additional testing of security control areas as required by DHS, OMB, CIGIE, and other oversight organizations.

## SCOPE

To accomplish our objective, we evaluated security controls in accordance with applicable legislation, presidential directives, and the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics Version 1.3,* dated April 9, 2019. 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 20 information systems (15 DOL and 5 DOL contractor information systems) from a total population of 63 information systems as of December 4, 2018. Our testing also included DOL-wide information security controls.

## METHODOLOGY

To assess the effectiveness of the information security program and practices of DOL, our procedures included the following:

- Inquired of information system owners, system administrators, and other relevant individuals to walk through each control process
- Inspected the information security practices and policies established by the Office of the Chief Information Officer.

- Inspected the information security practices, policies, and procedures in use across DOL
- Inspected the artifacts to determine the implementation and operating effectiveness of security controls
- Inspected results of vulnerability scanning results to determine the implementation of patches, logical access, and baseline compliance.

We performed our fieldwork at DOL's headquarters in Washington, District of Columbia during the period of February 5, 2019 through September 30, 2019. 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.[7] 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 essential to the development and implementation of agencies' security programs. We also utilized DOL's Computer Security Handbook, which outlines DOL's requirements for information security.

[7] The applicable AICPA standards are the Consulting Standards that require us to report to management our findings and recommendations.

# APPENDIX B: GLOSSARY

| ACRONYM | DEFINITION |
|---|---|
| Act, The | Title III of the E-Government Act of 2002 |
| AICPA | American Institute of Certified Public Accountants |
| CDM | Continuous Diagnostics and Mitigation |
| CIGIE | Council of the Inspectors General on Integrity and Efficiency |
| CIO | Chief Information Officer |
| CM | Configuration Management |
| CVE | Common Vulnerability Exposure |
| DHS | Department of Homeland Security |
| DOL | U.S. Department of Labor |
| DOLCSIRC | DOL Computer Security Incident Response Capability |
| FedRAMP | Federal Risk and Authorization Management Program |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Modernization Act |
| FY | Fiscal Year |
| ICAM | Identity, Credential, and Access Management Roadmap and Implementation Guidance |
| IG | Inspector General |
| ISCM | Information Security Continuous Monitoring |
| IT | Information Technology |
| KPMG | KPMG LLP |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| PII | Personally Identifiable Information |
| SP | Special Publication |
| US-CERT | United States Computer Emergency Readiness Team |

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

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

**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