U.S. Department of Labor

Office of Inspector General
Washington, DC. 20210

September 29, 2017

MEMORANDUM FOR: GUNDEEP AHLUWALIA
Chief Information Officer

Elliot P. Lewis

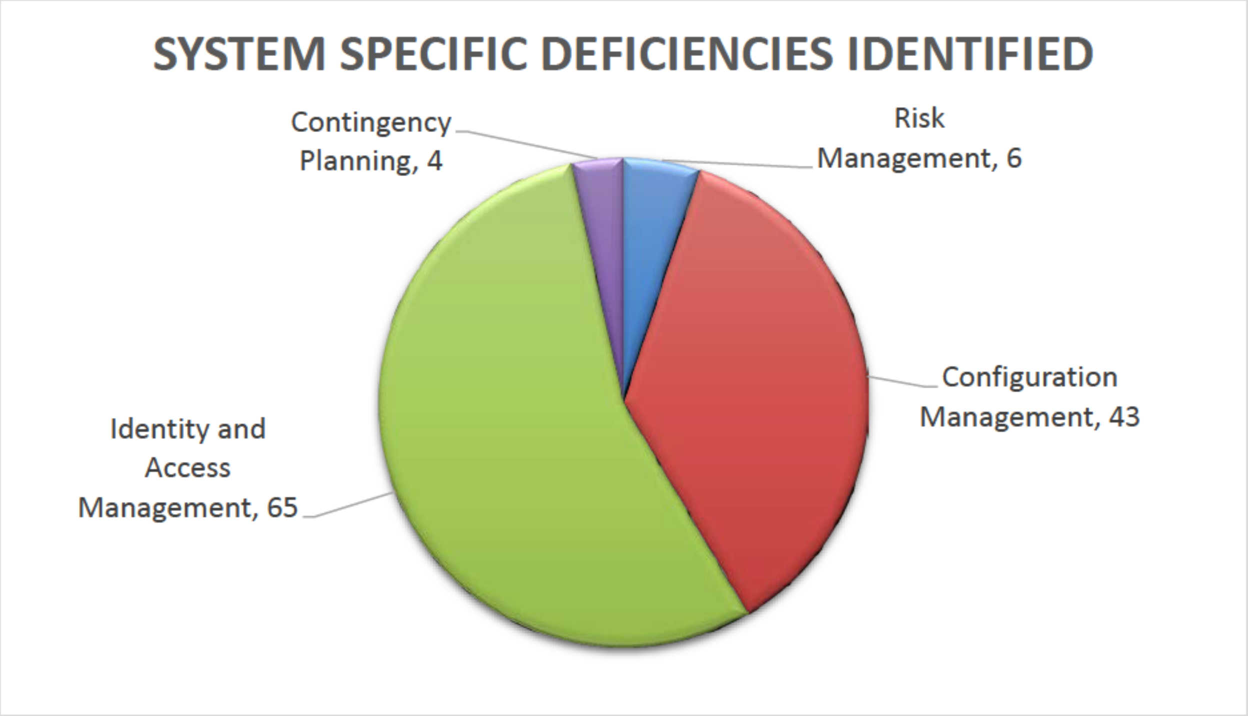
FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: FY 2016 FISMA DOL Information Security Report
Report Number: 23-17-002-07-725P

Attached is the Independent Auditors' Report on the U.S. Department of Labor's (DOL) Fiscal Year (FY) 2016 information security program and practices. We contracted with KPMG LLP (KPMG) to conduct this independent evaluation. DOL's Office of Inspector General (OIG) monitored KPMG's work to ensure it met professional standards and contractual requirements. We conducted the individual evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (CIGIE) 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 minimum information security program and practices for the period October 1, 2015, to September 30, 2016, for its information systems, including DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We based our work, in part, on a selection of DOL-wide security controls and a selection of system-specific security controls across 24 information systems (16 selected DOL information systems and 8 DOL contractor systems). We did not apply testing procedures to all information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope & Methodology*.

We identified 121 deficiencies in seven of the eight FISMA program areas. There were three entity-wide deficiencies in continuous monitoring, incidence response and reporting, and contractor systems. Additionally, as seen in the chart below, we identified 118 system specific deficiencies in the other program areas.



KPMG is responsible for the attached auditors' evaluation and the conclusions expressed in the report. However, in connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. This independent evaluation did not constitute an engagement in accordance with *Government Auditing Standards.*

The attached final report is submitted for your resolution action. In accordance with DLMS 8 – Chapter 500, paragraph 533, you should provide a written response within 60 days indicating your agency's agreement or disagreement with the recommendation. If you agree with the recommendation, your response should explain the planned corrective actions, identify officials responsible for such actions, and provide dates by which the actions will be taken and full implementation achieved. If you disagree with the recommendation, your response should fully explain the reasons for disagreement.

Should you have any questions, please contact Stephen Fowler, Information Technology Audit Director, at (202) 693-7010.

Attachment

cc: Edward C. Hugler, Deputy Assistant Secretary for Administration and Management
Tonya Manning, Acting Deputy CIO
Jason Tam, Acting Director, OCIO Information Assurance

Fiscal Year 2016 U.S. Department of Labor's Federal Information Security Modernization Act of 2014 Management Systems Report

September 27, 2017

KPMG LLP
1676 International Drive, Suite 1200
McLean, VA 22102

U.S. Department of Labor
Federal Information Security Modernization Act of 2014

Evaluation Table of Contents

KPMG LLP
1676 International Drive
McLean, VA 22102

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

Re: Fiscal Year 2016 U.S. Department of Labor's Federal Information Security Modernization Act Management Systems Report

This report presents the results of our independent evaluation for Fiscal Year (FY) 2016 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 the 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 2016 questionnaire to collect these responses. FISMA requires that the agency Inspector 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. The DOL Office of Inspector General (OIG) monitored our work to ensure we met professional standards and contractual requirements.

We conducted our 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 (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, 2015 to September 30, 2016 for its information systems, including the DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We assisted the DOL 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 24 information systems (16 selected DOL information systems, and 8 DOL contractor systems). Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope, Methodology and Criteria*.

DOL established its information security program and practices for its information systems in accordance with applicable FISMA requirements, OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines. DOL is maintaining a security program, which included the eight FY 2016 FISMA IG reporting domains[1].

While the security program has been implemented across DOL, we identified 121 deficiencies in the following seven of eight FISMA domains:

1. Risk Management
2. Contractor Systems
3. Configuration Management
4. Identity and Access Management
5. Information Security Continuous Monitoring
6. Incident Response and Reporting

[1] The eight FISMA metric domains are risk management, contractor systems, configuration management, identity and access management, security and privacy training, information security continuous monitoring, incident response and reporting, and contingency planning.

7. Contingency Planning

We recommended the CIO ensure the timely remediation of the deficiencies identified and previously provided to the relevant system’s management. In a written response, the DOL’s Chief Information Officer (CIO) agreed with our recommendations and provide actions they have taken and plan to take (see Management Response to the Report).

This independent evaluation did not constitute an engagement in accordance with Government Auditing Standards. KPMG did not render an opinion on the 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.

Appendix I describes the FISMA evaluation’s objective, scope, methodology, criteria. Appendix II contains acronyms and abbreviations of terms used in this report.

Sincerely,

KPMG LLP

September 27, 2017

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 the OMB, agency security policy, and NIST's risk-based standards and guidelines 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 several entities on the adequacy and effectiveness of agency information security policies and procedures. These include the OMB Director, the Comptroller General of the United States, and selected congressional committees. In "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) "(OMB Memo M-10-28), OMB delegated some responsibility to the DHS for operational aspects of Federal cyber security, 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 agency IG or an independent external auditor, as determined by the IG, should do the independent evaluation.

FISMA outlines that the CIO is responsible for:

- Developing and maintaining a [DOL-wide] information security program;

- Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;

- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;

- Ensuring agencies have trained personnel sufficient to assist [DOL] in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

- Reporting annually and in coordination with DOL agencies’ senior officials to the [Secretary] on the effectiveness of the agency information security program, including progress of remedial actions.

Section 811 of the Carl Levin and Howard P. ‘Buck’ McKeon National Defense Authorization Act for fiscal year (FY) 2015 amended the Clinger-Cohen Act by providing: explicit accountability to the CIO to manage all information technology (IT) resources. This includes approving: (1) the IT portion of the annual budget requests submitted to Congress; (2) all IT and IT service contracts; and (3) the appointment of any component- level Chief Information Officer.

OVERALL EVALUATION RESULTS

DOL established its information security program and practices for its information systems in accordance with applicable FISMA requirements, OMB policy and guidelines, and the National Institute of Standards and Technology (NIST) standards and guidelines. DOL is maintaining a security program for the five Cybersecurity Framework Security Functions that include eight FISMA metric domains. This is outlined in the Fiscal Year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3, September 26, 2016 that the DHS's Office of Cybersecurity and Communications Federal Network Resilience prepared[2]. The functions and domains were as follows:

- Identify
  - Risk management
  - Contractor systems
- Protect
  - Configuration management
  - Identity and access management
  - Security and privacy training
- Detect
  - Information security continuous monitoring
- Respond
  - Incident response
- Recover
  - Contingency planning

However, while the security program was implemented across the DOL, we identified 121 deficiencies that we reported to DOL management in seven of the eight FISMA metric domains. Without appropriate security, DOL may not be able to protect its mission assets. This puts the Agency's systems and the sensitive data they contain at risk. Some deficiencies we identified could negatively affect the confidentiality, integrity, and availability of the Agency's systems and personally identifiable information (PII). 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. DOL should make protection of its networks and information systems a top priority and dedicate resources needed to (1) ensure the appropriate design and operating effectiveness of information security controls and (2) prevent unauthorized access to sensitive information.

The *Findings* section of this report presents the detailed findings and associated recommendations. In a written response to this report, the DOL CIO agreed with our recommendations and provided actions they have taken and plan to take (see Management Response). DOL's planned corrective actions are responsive to the intent of our recommendations.

[2] The scoring methodology is described in this document and the scoring is determined by the entries DOL entered into CyberScope

FINDINGS

1. Risk Management

Thirteen of 13 systems tested revealed Risk Management control deficiencies related to system interconnections, POA&Ms, system security plans, and risk assessments. Specifically, as depicted in Table 1 below, we identified six deficiencies in the areas of System Interconnections, Plan of Action and Milestones, Plan of Action and Milestones Process, System Security Plan, & Risk Assessment.

Table 1: Risk Management Issues Resulted in Deficiencies

NIST Criteria	Control Name	Number of Deficiencies and System(s)
6 Risk Management Deficiencies		
CA-3	System Interconnections	1 Deficiency in 1 system
PM-4; CA-5	Plan of Action and Milestones; Plan of Action and Milestones Process	3 Deficiencies in 13 systems
PL-2; RA-3	System Security Plan; Risk Assessment	2 Deficiencies in 2 systems

Plan of Action and Milestone Deficiencies
DOL did not review and monitor Plan of Action and Milestones (POA&Ms) timely within the required 45 days after the end of the quarter for 13 information systems (see Table 1, PM-4 and CA-5 NIST Criteria.) Specifically, DOL performed bi-annual reviews of POA&Ms according to DOL policy but did not perform OMB-mandated quarterly reviews of POA&Ms submitted by the agencies. The agencies are required to manage their POA&Ms and are aware of remediation actions and planned scheduled mitigation dates. For remediation testing of 102 POA&Ms marked as “closed,” only 9 were actually “closed” and testing determined that DOL did not complete corrective action plans sufficiently in order to close the remaining POA&M.

Volume 4 of the DOL Computer Security Handbook (CSH), last reviewed in May 2015, states:

> POA&Ms are to be updated on a continual basis and will be reviewed by the OCIO Security at least semi-annually. The OCIO Security Calendar provides the schedule as to the cutoff date for POA&M updates for a given quarter. OCIO semi-annual reviews will be completed and a CSAM POA&M report generated for the systems reviewed (typically within the next 30 calendar days after the cutoff date) providing a snapshot by system. OCIO security will review all POA&M reports for the designated quarter and, after confirmation of the findings

by agencies, generate a report card with comments and upload the document as an artifact into CSAM.

OCIO stated that it did not post semi-annual scorecards and quarterly snapshots timely to CSAM because of competing department priorities.

When the agencies are not informed of the results of the POA&M review in a timely manner, the completeness and accuracy of agencies' POA&Ms and remediation actions unnecessarily places DOL systems at risk through the lack of remediation monitoring efforts. Without appropriate monitoring, POA&Ms related to remediating control deficiencies may not be acted upon within an acceptable amount of time. Therefore, agencies may not be taking steps to remediate identified weaknesses, which could affect the confidentiality, integrity, and availability of information system data.

System Security Plan, Risk Assessment, and System Interconnection Deficiencies

OASAM did not review SSP and Risk Assessment documents for two of its systems. OASAM management stated that it did not review one of its system's SSP and Risk Assessment in FY 2016 because of a delay in the migration to NIST SP 800-53 Rev. 4 security controls. The system also still had not completed a memorandum of understanding (MOU) and interagency security agreement (ISA) between it and the General Service Administration's (GSA) System for Award (SAM) because DOL and GSA were still reviewing the documents. The agency attributed the delay to a dispute with the system vendor over contractually-mandated support levels. ETA management stated it did not upload a system's SSP and Risk Assessment documents to CSAM due to lack of edits made to the documents.

2. Contractor Systems

Eight of 8 contractor systems tested identified that system owners were not monitoring third party providers' compliance with DOL security requirements for cloud systems (CA-2 NIST Criteria). Similar deficiencies reoccurred in the past three years. This shows that the OCIO had not effectively implemented monitoring controls related to cloud system providers.

Our testing determined that although DOL developed and maintained Volume 15 of the DOL CSH, which includes language about Third Party Monitoring and Oversight, the policy excluded agency third-party cloud system oversight. Additionally, DOL's Third Party Monitoring Guide states that OCIO Security works with DOL agencies and third party service providers to review critical unresolved issues between both parties. Furthermore, DOL agencies should complete a third party compliance review, including the development of a Corrective Action Plan to address and mitigate any risks, and provide it to the third party service provider. Providing guidance to designated personnel and monitoring the oversight of these third-party systems, while excluding cloud system providers, poses risks. For example, the likelihood increases that the system's security posture would not be consistently reported to the authorizing officials. As a result, DOL would not know if the third party systems complied with mandatory security requirements.

3. Configuration Management

Fifteen of 16 information systems tested had deficiencies associated with configuration management.

Specifically, DOL has no formal processes for maintaining an inventory of all hardware, software, and applications at the Department. Inventory information is part of the agency system security plan and stored in CSAM.

Additionally, management could not provide evidence that it scanned baseline configurations on a quarterly basis. Management could not provide baseline security checklists for the following operating systems: Windows Server 2008, Cisco Router, Cisco Firewall, UNIX, and AIX because DOL has not documented baseline security checklists for devices connected on the network. Specifically, we identified 43 total deficiencies within the areas of Continuous Monitoring & Vulnerability Scanning, Baseline Configuration, Information System Component Inventory, and Flaw Remediation, Configuration Settings, & Unsupported System Components.

The system deficiencies related to configuration management are provided in Table 3 below.

Table 2: Configuration Management Issues Resulted in Deficiencies

NIST Criteria	Control Name	Number of Deficiencies and System(s)
43 Configuration Management Deficiencies		
CA-7; RA-5	Continuous Monitoring; Vulnerability Scanning	24 Deficiencies in 12 systems
CM-2	Baseline Configuration	2 Deficiencies in 2 systems
CM-8	Information System Component Inventory	1 Deficiency in 1 system

NIST Criteria	Control Name	Number of Deficiencies and System(s)

SI-2;
CM-6;
SA-22
	Flaw Remediation;
	Configuration Settings;
	Unsupported System Components
		16 Deficiencies in 7 seven systems

Operating System Patch Management

Eight of 16 systems tested (see table 2, CA-7, RA-5, SI-2, CM-6, SA-22 NIST Criteria), did not have critical operating system patches installed in a timely manner. For operating system servers, we determined that the vendor released the most recent critical patch in May of 2016, but the patch was not implemented on any of the in-scope hosts at the end of FY 2016.

We noted for two system in one of DOL's agencies that follows the quarterly patch distribution process that is released every January, April, July and October. One system had, 8 Critical, 9 High and 20 Medium and the other had 12 Critical, 14 High and 30 Medium patches came out after the quarterly patch cluster in July 2016 and were scheduled for update in October 2016.

For one system, we noted the OCIO continuous monitoring program did not proactively enforce the identification of security risks and mitigation of IT assets. Specifically, the continuous monitoring program did not consistently enforce routine patch management, vulnerability scanning, and remediation to protect against vulnerability threats identified using organizational deployed assessment tools.

Volume 17 of the DOL CSH states that OCIO security reserves the right to specify a minimum level of importance (including, but not limited to, minimum requirements) for updates that approved sources have released. 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 must be installed within 72 hours of release;
b) Updates identified as high importance must be installed within five business days of release;
c) Updates identified as moderate importance must be installed within 10 days of release; and

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

According to OASAM management, the O/S versions had not been upgraded in a timely manner because of resource constraints. DOL management explained that newer patches were impacting business performance and funding was not provided to upgrade certain software projects.

Untimely implementation of security updates or patches increases the risk of a compromise of the confidentiality, integrity, and availability of the financially relevant data residing on the information systems.

Database System Patch Management

Eight of 16 systems tested (see table 2, SI-2, CM-6, and SA-22 NIST Criteria), did not have critical database system patches installed in a timely manner. Specifically, we determined that the databases supporting the four applications were running an outdated version, which has been unsupported by the vendor since April 30, 2015. Additionally, the database supporting a different application was running an outdated version, which has been unsupported by Oracle since July 2015.

Volume 17 of the DOL CSH states that OCIO security reserves the right to specify a minimum level of importance (including, but not limited to, minimum requirements) for updates 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 must be installed within 72 hours of release;
b) Updates identified as high importance must be installed within five business days of release;
c) Updates identified as moderate importance must be installed within 10 days of release; and
d) Updates identified as low importance must be installed within 20 business days of release.

OASAM management stated that the database versions for four systems have not been upgraded because of funding issues. They also noted that the OCIO was unable to patch to newer releases in the other database because business operating requirements prevented a full-scale upgrade of the database. Space and performance-related issues contributed to further delays in patching. DOL management explained that newer patches impacted business performance and there was no funding to upgrade certain software projects.

Untimely implementation of security updates or patches increases the risk of a compromise of the confidentiality, integrity, and availability of the financially relevant data residing on the information systems.

Configuration Standard Review and Monitoring was not Consistently Implemented

Seven of 16 systems tested (see table 2, SI-2, CM-6, and SA-22 NIST Criteria), did not have consistent implementation of configuration review and monitoring. While management had a list of known deviations, they did not provide a reason for the deviations or an explanation of related mitigating controls. We determined checklists were provided; however, deviations were not fully documented for certain servers, and management was not able to provide evidence that baseline configurations were scanned on a quarterly basis.

In addition, management was not able to provide baseline security checklists for other operating systems. DOL provided no evidence that management groups were provided baseline compliance and CVE reports for review and correction on a monthly or quarterly basis. Furthermore, DOL has not implemented a security tool to check for outdated patches of non-Microsoft based assets and DOL has a resource constraint to monitor and apply patches to impacted assets.

Finally, DOL also has not implemented an automated process for maintaining an inventory of all software and hardware connected to the DOL network. DOL's process is to manually assemble information provided by the agencies and sent to OCIO. There is no automation in the process nor verification of the inventory components. The aforementioned conditions do not adhere to Volume 5 of the DOL CSH. The CSH states:

[The] system owner or information system personnel authorized by the system owner shall:

> a) Agencies must establish and implement configuration settings for information technology products employed within the information system using agency-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements. The configuration settings must comply with the procedures and standards set forth by the Department (including but not limited to, CSH, and NIST guidelines for applicable technologies;
> b) Identifies, documents, and approves any deviations from established configuration settings for agency-defined hardware, software, or firmware components based on explicit operational requirements.

Without performing baseline configuration scans on a regular basis against documented and approved baselines, management is unable to ensure that configurations are being maintained at their required settings, which could negatively impact controls around confidentiality, availability, and accuracy of data.

Vulnerability Scanning

Eleven of 16 systems tested (see table 2, CA-7 and RA-5 NIST Criteria), had critical, high, and medium vulnerabilities identified as a result of vulnerability scanning.

OCIO stated that an enterprise-wide vulnerability tool was not fully implemented during FY 2016. The OCIO is working with relevant agencies to establish a vulnerability management process to perform routine scans. Specifically, Volume 17 of the DOL CSH states:

> DOL information systems must identify, report, and correct information system flaws; relevant security updates 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 the ODHS Security on a monthly basis; Agencies must monitor for vulnerability and/or patch releases.

Without a fully implemented enterprise-wide vulnerability tool, the ability to detect and monitor vulnerabilities is limited, which could lead to a compromise of the confidentiality, integrity, and availability of data residing on the information system.

4. Identity and Access Management

Eleven of the 16 systems tested included pervasive Identify and Access Management deficiencies in 2016. Specifically, there were 65 total deficiencies within the areas of Account Management, Maintenance Personnel, Personnel Termination, Rules of Behavior (ROB), Security Awareness, Separation of Duties, Audit Events, Audit Review, Analysis and Reporting, Protection of Audit Information, Identification and Authentication, Authenticator Management, and Session Lock. Table 3 provides more details on the specific systems and their identity and access management deficiencies.

Table 3: Identity and Access Management Issues Resulted in Deficiencies

NIST Criteria	Control Name	Number of Deficiencies and System(s)
65 Identity and Access Management Deficiencies		

AC-2;
MA-5;
PS-4;
PL-4;
AT-2
	Account Management;
	Maintenance Personnel;
	Personnel Termination;
	Rules of Behavior;
	Security Awareness
		30 Deficiencies in 13 systems

AC-5	Separation of Duties	5 Deficiencies in 4 systems

AU-2;
AU-6;
AU-9
	Audit Events;
	Audit Review, Analysis and Reporting;
	Protection of Audit Information
		18 Deficiencies in 8 systems

IA-2	Identification and Authentication	1 Deficiency in 1 system

NIST Criteria	Control Name	Number of Deficiencies and System(s)
IA-5; AC-11	Authenticator Management; Session Lock	4 Deficiencies in 2 systems
PL-4	Rules of Behavior	6 Deficiencies in 6 systems
PS-4	Personnel Termination	1 Deficiency in 1 system

Account Management Testing Revealed User Accounts Active After User Termination

Eight of 17 systems tested included user accounts for terminated individuals that were not removed timely and were not deactivated after a period of inactivity. We also found three user accounts that were accessed after the termination date of the user. We noted that Volume 13 of the DOL CSH states:

> When employment is terminated, the agency shall: Disabled information system access within the 24 hours of that employee's separation when termination is voluntary; and disable information system access within four (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).

These deficiencies occurred because DOL uses a manual process for submitting forms for separated users. The manual process increases the risk that forms are not submitted timely, not submitted, or lost. Additionally, DOL does not centrally track contractors. DOL also stated that scripts used to disable/remove access had been suspended. Removing access to user accounts as soon as individuals are terminated eliminates the risk of unauthorized access. Instead, accounts for these terminated users were either currently active as of testing or had been active for a period of time after the users' termination dates. When accounts of terminated and inactive users are not removed or disabled in a timely way, unacceptable risks result, such as compromise of Department information or data.

Account Recertification Not Performed Correctly

Six of 17 systems tested contained user accounts that were not recertified appropriately, Recertification allows supervisors to review access of individuals that report to them and inform the system owner if the access should be removed, modified, or if no change is needed. While system owners performed recertification, they did not review the

individual's assigned roles or privileges because this information was not included for recertifying officials.
According to Volume 1 of the DOL CSH:

> Information system accounts (agency determined sample based on assessment of risk) must be reviewed every six months to also include the matching of user accounts with relevant user records (including but not limited to, personnel files) to ensure that terminated or transferred individuals do not retain system access. Note: the annual recertification of accounts must be a full review of all user accounts.

The system owners did not know the requirements to perform account recertification. Failure to do these reviews as required or at an increased frequency increases the risk that unauthorized access could exist if the individuals no longer need access to the information systems.

Systems Lacked Separation of Duties

Four of 17 systems tested contained users with granted roles that violated separation of duties. Additionally, one of 17 systems did not have an associated, formally authorized, separation of duties matrix. Furthermore, DOL stated that third service providers did not adhere to DOL requirements or make the requested changes to be compliant with Volume 1 of the DOL CSH. The CSH states:

> Separate duties of general and privileged users as necessary to prevent malevolent activity without collusion; Document separation of duties of individuals; and define information systems access authorizations to support separation of duties.

Management of the service organization indicated that the privileges described are necessary because of the limited number of personnel available to provide full-time support to the database. ETA and OASAM management stated that a user had the ability to give himself access to any role in the application. The user granted himself access to a role in order to "troubleshoot" application issues, which is one of his job functions, and never had his access removed appropriately. Additionally, there were no documented procedures to mitigate the risk posed by a technical user's access to troubleshoot issues in the application. Segregation of duties deficiencies raises the risk of unauthorized individuals being afforded unchecked opportunities for abuse, including, but not limited to, introducing fraudulent data or malicious code into the system.

Systems Did Not Follow Rules of Behavior / Access Agreements

Responsible agencies for eleven of 17 systems tested did not complete, document, or perform new user access authorizations, related rules of behavior forms, and/or user recertification. According to Volume 12 of the DOL CSH:

> DOL agencies must receive signed acknowledgement from user indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access information and the information system; Review and update the rules of behavior annually or whenever a significant change to the system occurs; and require individuals who have signed a previous version of the ROB to read and resign when the ROB is revised or updated.

OCIO stated that they could not provide documentation for the ROB acknowledgement for the listed users because the paper-based documentation for users with existing accounts has not been tracked effectively over the years. Additionally, the OCIO does not collect ROBs in a central location. Without obtaining and maintaining record of users' acknowledgement of the Rules of Behavior, DOL does not have assurance that users are aware of their responsibility in regards to DOL application information and information systems.

Generic Active Accounts Prohibited by DOL Policy

One of the 17 systems tested had 77 of 84 active database accounts that were generic and, thus, prohibited by DOL policy. DOL policy requires unique, as opposed to generic, user accounts so that the agency can identify an individual user and hold them accountable for any actions taken from that account or process. Volume 7 of the DOL CSH prohibits generic user accounts. The CSH states, "Shared user accounts (including but not limited to, generic, administrator, guest, and temporary) are not permitted". OASAM management informed us that they did not have resources to research the system accounts. OASAM management also indicated that they are working on identifying business purposes for the aforementioned accounts, but we were unable to assess their efforts at year-end. When prohibited generic accounts were used to access the database, it would be impossible to determine the identity of the processors, or review which individual had processed, specific grant-related data. Therefore, program agency management would not be able to determine accountability for specific actions in the system.

Password Configuration Settings

Two of the 17 systems tested contained password configuration setting deficiencies related to established parameters (i.e., password composition, length, life, history) that the system used to identify who has access to the system. These password settings ensure enforcement of requirements (such as changing passwords periodically) that make it hard to gain access by guessing another user's password.

> For one system the application, database, and operating system password configurations were not configured in accordance with the settings outlined in the DOL CSH, Volume 7, Edition 5.0, *Identification and Authentication Policies, Procedures, and Standards*.
>
> For the other system the application, database, and operating system password

configurations were not configured in accordance with the settings outlined in the DOL CSH, Volume 7, Edition 5.0, *Identification and Authentication Policies, Procedures, and Standards*.

OASAM management stated that password settings cannot be changed without concurrence of the system owner since it would impact system operation. However, there are plans to change them once DOL implements new hardware and software in early FY 2017. Furthermore, password settings were not updated timely because there was high turnover of individuals that support the system. When DOL does not configure user account security in accordance with the DOL CSH, there is a greater risk of unauthorized individuals gaining access to grant and non-public unemployment data. Additionally, potential user accounts have access to pre-public release information with significant impact and risk to economic markets.

Audit and Accountability

Eight of the 17 systems tested included existing audit and accountability control deficiencies. Seven systems did not document their audit log reviews as required by DOL policy. Also, the log aggregate tool was operational, but not used because of a related software license that expired in FY 2015. Additionally, 3 of 17 information systems tested did not periodically review users with privileged access as required by Volume 3 of the DOL CSH. The CSH states:

> 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.

Additionally, Volume 3 of the DOL CSH states:

> DOL's required minimum standards on managing information system audit events are as follows; 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 permissions executed on user accounts;
> c. administrative permissions executed on a system resource;
> 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; and
> g. all computer-readable data extracts from databases containing personally identifiable information.

OASAM management stated that the security information and event management (SIEM) tool was decommissioned in FY 2015 and they did not have sufficient data storage to accommodate the audit logs. Without the ability to gather or review audit logs, systems were at an increased level of risk for fraudulent activities that might compromise data.

Without proper and timely review of audit logs, OASAM could not identify unauthorized access or activity in applications.

5. Information System Continuous Monitoring

In FY2016, DHS and OMB asked the OIG to assess the Department's continuous monitoring process (NIST Criteria CA-5) based on a five-scale maturity model evaluating the people, processes, and technology within the Department as it pertains to information security continuous monitoring[3]. The five levels specified in Appendix III include: Level 1: Ad-hoc; Level 2: Defined; Level 3: Consistently Implemented; Level 4: Managed and Measurable; and Level 5: Optimized.

For a Level 2: Defined organization, DOL has defined the stakeholders of the ISCM program, what skills are needed and the gaps that currently exist for individuals that support the ISCM program, shared ISCM information with individuals with significant security responsibilities, and tied DOL ISCM activates to DOL's Enterprise Risk Management Strategy (ERMS).

However, DOL had the following gaps in the ISCM program process:

- DOL did not implement controls or tools to address ongoing assessments and monitoring of security controls;
- DOL did not perform hardware asset management or software asset management;
- DOL did not perform configuration setting management or common vulnerability management;
- DOL did not collect security related information required for metrics, assessments, and reporting, nor analyze ISCM data for reporting findings and determining the appropriate risk responses; and
- DOL did not define qualitative and quantitative performance measures that would allow them to share information among stakeholders**.**

[3] The ISCM maturity model is described in described in the Fiscal Year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3, September 26, 2016 on pages 10 – 17.

6. Incident Response and Reporting

In FY16, DHS and OMB asked the OIG to assess the Department's incident response and reporting process (NIST Criteria IR-6) based on a five-scale maturity model evaluating the people, processes, and technology within the Department as it pertains to incident response and reporting[4]. The five levels specified in Appendix IV include: Level 1: Ad-hoc; Level 2: Defined; Level 3: Consistently Implemented; Level 4: Managed and Measurable; and Level 5: Optimized

DOL has an ad-hoc IRR program. We found that DOL:

- Did not consistently define elements of incident response such as which skills are needed and the gaps that currently exist for individuals that support the IRR program;
- Did not define how the organization will handle incident detection, analysis, containment, eradication, and recovery;
- Did not define how the organization will handle documentation of trend analysis, situational awareness, or control of ongoing risk; and
- Did not document how the organization will make use of incident response tools such as web application protections, event and incident management, aggregation and analysis, malware detection, information management, file integrity, and endpoint server security.

We determined that a number of incidents were not reported from the applicable agency to the DOLCSIRC team within one day. We also found that DOLCSIRC failed to report a number of cyber incidents to the United State Computer Emergency Readiness Team (US-CERT) within one business day as required. This condition does not adhere to criteria in Volume 8 of the DOL CSH. The CSH states:

> DOLCSIRC shall report the incident to the OIG, US-CERT, Office of Public Affairs (OPA), the DOL Physical Security Officer, and DOL Senior Management, as appropriate; and Incident reports must be submitted to DOLCSIRC via e-mail to dolcsirc@dol.gov. Confirmed incidents need to be reported within the same business day. To ensure timely reporting, agencies can also notify DOLCSIRC via phone of an incident however agencies can also submit a DOLCSIRC incident reports form following the verbal notification.

OASAM management stated that the agencies did not report the 47 incidents to DOLCSIRC in a timely manner because they were unaware of the timeframe required to report the incident. In addition, OASAM management stated that the six cyber incidents were not reported timely from DOLCSIRC to US-CERT because they either had to be reviewed and verified to ensure they warranted submission to US-CERT, or DOLCSIRC staff were unaware of the timeframe required to report the incident. Not reporting an incident timely could result in actions to detect and protect against malicious code or other

[4] The ISCM maturity model is described in described in the Fiscal Year 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3, September 26, 2016 on pages 18 – 21.

critical DOL information and systems being delayed, allowing those systems and information to be compromised.

7. Contingency Planning

Three of 16 information systems tested found that contingency planning was not operating as intended. These deficiencies included backup procedures and documentation of alternate sites. Specifically, as Table 4 indicates, there were four total deficiencies within the areas of Information System Monitoring, Alternate Storage Site, Alternate Processing Site, and Information System Backup.

Table 4: Contingency Planning Issues Resulted in Deficiencies

NIST Criteria	Control Name	Number of Deficiencies and System(s)
4 Contingency Planning Deficiencies		
SI-4	Information System Monitoring	1 Deficiency in 1 system
CP-6; CP-7	Alternate Storage Site; Alternate Processing Site	1 Deficiency in 1 system
CP-9	Information System Backup	2 Deficiencies in 2 systems

Alternate Processing Sites Not Identified

One of 16 information systems tested utilized an alternate site location without defined security processing controls as required by DOL CSH Edition 5.0, Volume 6, *Contingency Planning Policies, Procedures, and Standards,* dated May 2, 2014.

The high turnover rate within the team responsible for consolidating alternate processing sites among program agency systems relying on the system led to problems. This included miscommunication of responsibilities. The inability to identify an alternate processing site for moderate risk systems would mean that systems would not meet their Recovery Time Objective (RTO) and availability requirements. Consequently, DOL would not be able to fulfill its essential business missions and functions, such as supporting the system that aids the Employee Benefits Security Administration (EBSA) in their day-to-day activities.

Aborted Information System Backups Were Not Re-performed

Two of 16 systems tested reported backups with an “aborted status” that were not confirmed by management as having run successfully. Volume 6 of the DOL CSH states:

> Information system personnel shall conduct backups of user-level information contained in the information system daily for incremental data and weekly for all data.

There was a job scheduling conflict, which resulted in incomplete backups and the backup software did not show that the job was completed successfully. Without performing information system backups in a timely manner, DOL increases the risk that data residing within the information system would not be restored in the event of data corruption or loss. Historical and current grant information and unemployment data could be lost, which would cause delays in providing services to the impacted recipients.

Lack of Information System Monitoring

One of 16 systems tested did not have system monitoring capabilities enabled for 4 months under audit. Additionally, alerting capability was not activated until 6 months under audit. This meant that system administrators received no system monitoring alerts for 6 months. An inspection of service tickets found that servers supporting the system did not have any processing failures during this six month period.

Recommendation

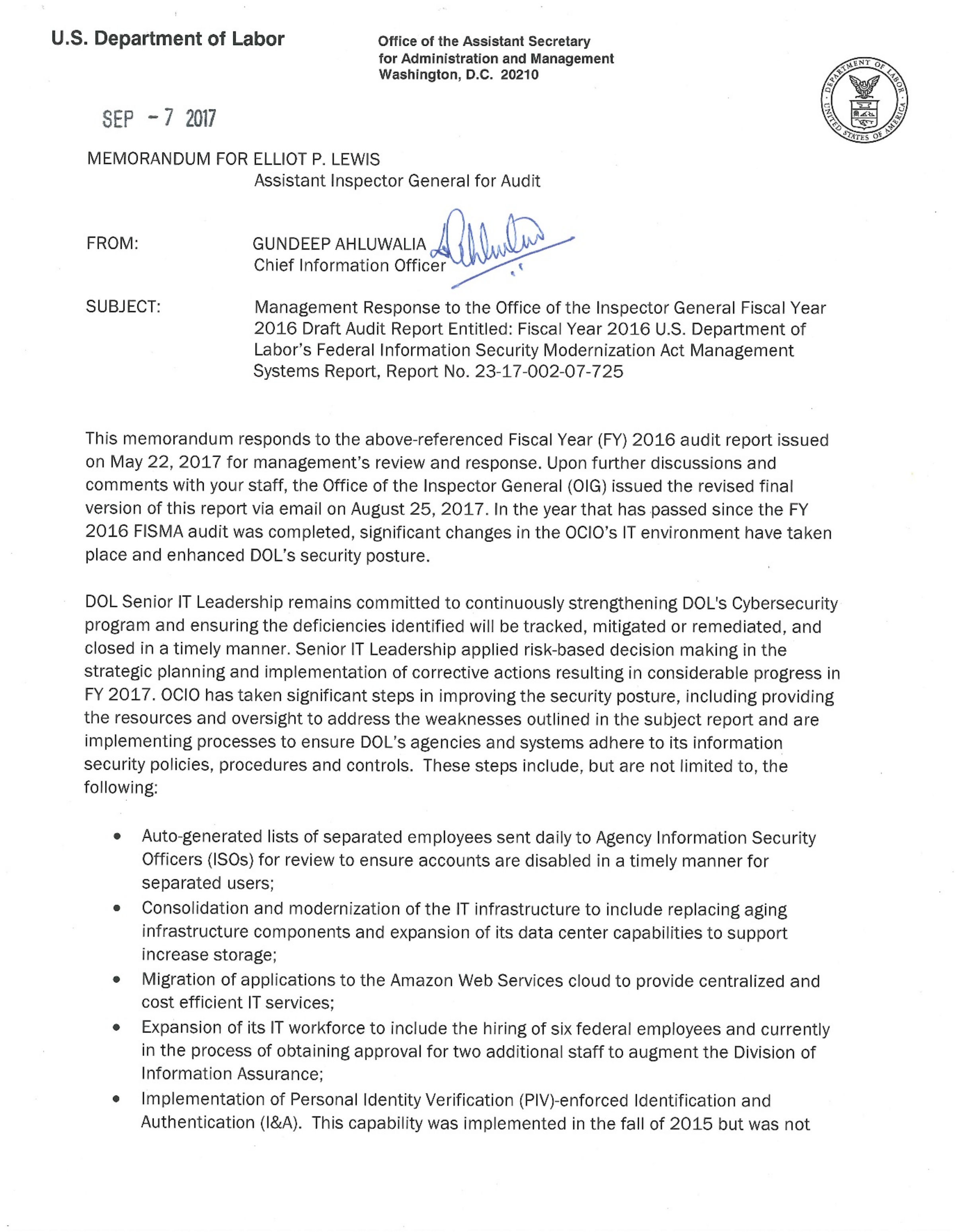
Although DOL established an information security program and practices across the Agency, we identified numerous deficiencies that may limit the Agency's ability to adequately protect the organization's information, PII, and information systems. Without appropriate security, DOL may not be able to protect its mission assets adequately. As such, the Agency's systems, and the sensitive data they contain are at risk. We identified deficiencies that could negatively affect the confidentiality, integrity, and availability of the Agency's systems and PII. To be consistent with FISMA, the CIO should provide the resources and oversight to address these weaknesses; and ensure DOL’s agencies and systems adhere to its information security policies, procedures and controls.

We recommend the Chief Information Officer:

Ensure the deficiencies identified are provided to agency management and they are remediated and closed in a timely manner.

MANAGEMENT RESPONSE TO THE REPORT

The following is the DOL CIO’s response, dated September 7, 2017, to our draft FY 2016 FISMA Evaluation Report the DOL OIG provided on May 22, 2017, and a revised draft report provided on August 25, 2017.



U.S. Department of Labor

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

SEP - 7 2017

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

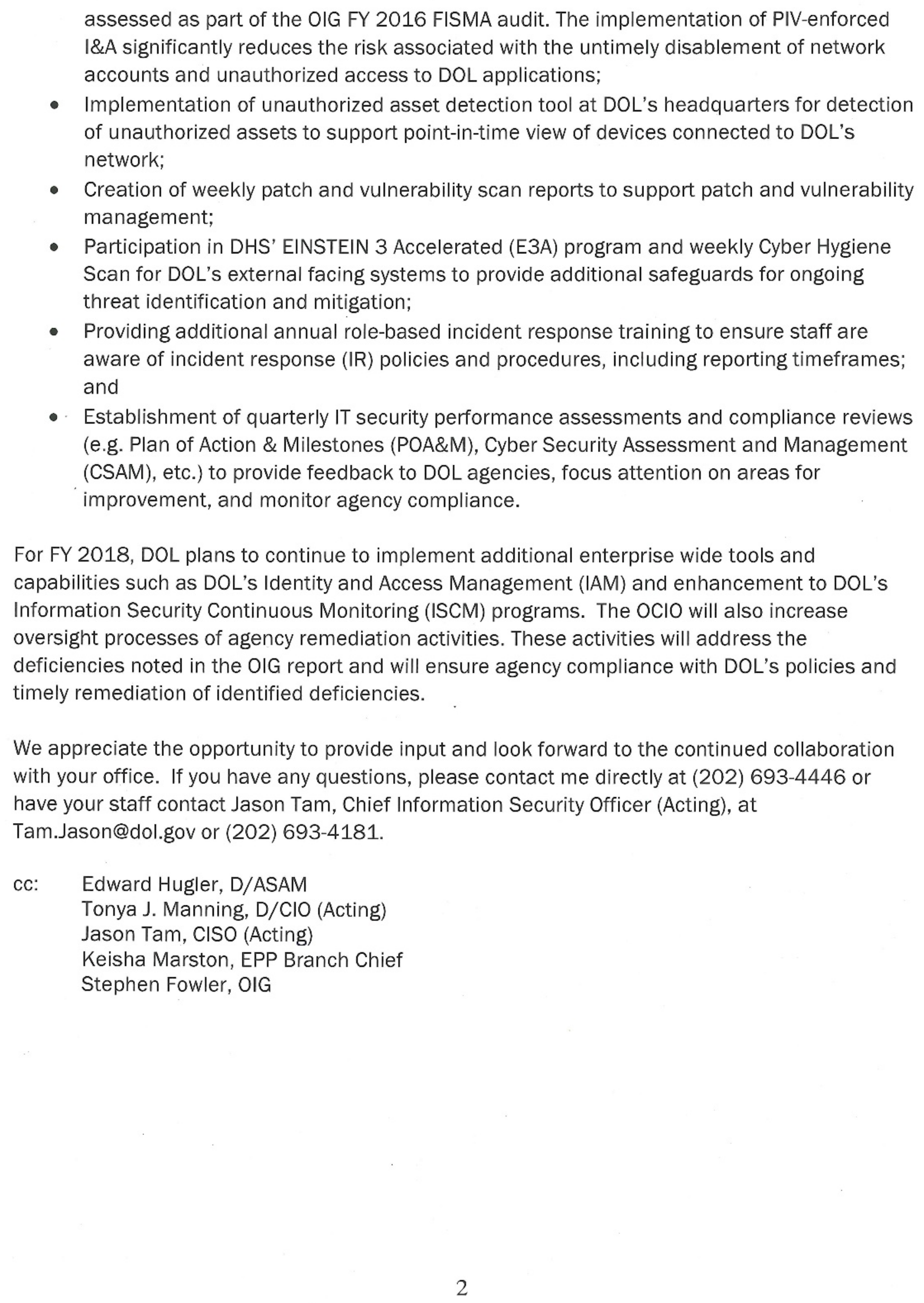
FROM: GUNDEEP AHLUWALIA
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2016 Draft Audit Report Entitled: Fiscal Year 2016 U.S. Department of Labor's Federal Information Security Modernization Act Management Systems Report, Report No. 23-17-002-07-725

This memorandum responds to the above-referenced Fiscal Year (FY) 2016 audit report issued on May 22, 2017 for management's review and response. Upon further discussions and comments with your staff, the Office of the Inspector General (OIG) issued the revised final version of this report via email on August 25, 2017. In the year that has passed since the FY 2016 FISMA audit was completed, significant changes in the OCIO's IT environment have taken place and enhanced DOL's security posture.

DOL Senior IT Leadership remains committed to continuously strengthening DOL's Cybersecurity program and ensuring the deficiencies identified will be tracked, mitigated or remediated, and closed in a timely manner. Senior IT Leadership applied risk-based decision making in the strategic planning and implementation of corrective actions resulting in considerable progress in FY 2017. OCIO has taken significant steps in improving the security posture, including providing the resources and oversight to address the weaknesses outlined in the subject report and are implementing processes to ensure DOL's agencies and systems adhere to its information security policies, procedures and controls. These steps include, but are not limited to, the following:

- Auto-generated lists of separated employees sent daily to Agency Information Security Officers (ISOs) for review to ensure accounts are disabled in a timely manner for separated users;
- Consolidation and modernization of the IT infrastructure to include replacing aging infrastructure components and expansion of its data center capabilities to support increase storage;
- Migration of applications to the Amazon Web Services cloud to provide centralized and cost efficient IT services;
- Expansion of its IT workforce to include the hiring of six federal employees and currently in the process of obtaining approval for two additional staff to augment the Division of Information Assurance;
- Implementation of Personal Identity Verification (PIV)-enforced Identification and Authentication (I&A). This capability was implemented in the fall of 2015 but was not



assessed as part of the OIG FY 2016 FISMA audit. The implementation of PIV-enforced I&A significantly reduces the risk associated with the untimely disablement of network accounts and unauthorized access to DOL applications;

- Implementation of unauthorized asset detection tool at DOL's headquarters for detection of unauthorized assets to support point-in-time view of devices connected to DOL's network;
- Creation of weekly patch and vulnerability scan reports to support patch and vulnerability management;
- Participation in DHS' EINSTEIN 3 Accelerated (E3A) program and weekly Cyber Hygiene Scan for DOL's external facing systems to provide additional safeguards for ongoing threat identification and mitigation;
- Providing additional annual role-based incident response training to ensure staff are aware of incident response (IR) policies and procedures, including reporting timeframes; and
- Establishment of quarterly IT security performance assessments and compliance reviews (e.g. Plan of Action & Milestones (POA&M), Cyber Security Assessment and Management (CSAM), etc.) to provide feedback to DOL agencies, focus attention on areas for improvement, and monitor agency compliance.

For FY 2018, DOL plans to continue to implement additional enterprise wide tools and capabilities such as DOL's Identity and Access Management (IAM) and enhancement to DOL's Information Security Continuous Monitoring (ISCM) programs. The OCIO will also increase oversight processes of agency remediation activities. These activities will address the deficiencies noted in the OIG report and will ensure agency compliance with DOL's policies and timely remediation of identified deficiencies.

We appreciate the opportunity to provide input and look forward to the continued collaboration with your office. If you have any questions, please contact me directly at (202) 693-4446 or have your staff contact Jason Tam, Chief Information Security Officer (Acting), at Tam.Jason@dol.gov or (202) 693-4181.

cc: Edward Hugler, D/ASAM
Tonya J. Manning, D/CIO (Acting)
Jason Tam, CISO (Acting)
Keisha Marston, EPP Branch Chief
Stephen Fowler, OIG

APPENDIX I – Objective, Scope, Methodology and Criteria

OBJECTIVE

Did DOL implement effective FISMA minimum information security requirements?

SCOPE

Using the Office of Management and Budget / Department of Homeland Security metrics, National Institute of Standards and Technology guidance, and DOL policies and procedures, we tested 24 systems in FY 2016 from a reportable FISMA system inventory of 72 systems. This included 16 DOL systems and eight contractor systems. We selected a subset of DOL systems and NIST SP 800-53 Revision 4 security control areas using a risk-based approach for testing. KPMG performed a risk assessment of the DOL FISMA reportable information systems to make a representative select of information systems to perform our evaluation procedures to determine if DOL implemented effective security controls. We also include in our selection of information systems financial relevant systems that were part of our scope of the financial statement audit.

The control tests included reviews of DOL agency policies and procedures for implementing and monitoring mandatory information security controls, as well as implementation of the mandatory controls for DOL agency systems. Based on OMB/DHS criteria, we tested selected controls in the DOL Cyber Security Program from the following 8 security control areas:

1) Identify – Risk Management
2) Identify – Contractor Systems
3) Protect – Configuration Management
4) Protect – Identity and Access Management
5) Protect – Security and Privacy Training (Entity-Wide)
6) Detect – Information Security Continuous Monitoring (Entity-Wide)
7) Respond – Incident Response and Reporting (Entity-Wide)
8) Recover – Contingency Planning

METHODOLOGY

This project followed a phased approach including planning, testing, and reporting as discussed below.

Planning

We reviewed DOL's policies and procedures, as well as applicable federal laws, guidelines, and requirements. We obtained and examined DOL information security policies, procedures, and controls for selected DOL major information systems, including related third-party systems. We examined these elements in order, to: (1) understand and become familiar with the DOL information security control environment; (2) facilitate the planned process of assessing both the effectiveness of selected information security controls; and (3) determine the extent of DOL compliance with minimum information security and FISMA requirements.

We planned our work in order to provide OMB with results on the effectiveness of DOL's cyber security program, and to notify the OCIO of any design and operating deficiencies identified under agency and DOL key information security controls. We planned to both summarize the work performed in answering the OMB IG Reporting Template, and provide additional information and analyses regarding information security deficiencies identified in DOL.

We used a risk-based approach to select our subset of information systems from DOL's inventory of major information systems.

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS FY 2016 Inspector General Federal Information Security Modernization Act Reporting Metrics, dated June 20, 2016.

We mapped the requirements of FY2016 DHS/OMB questions to the NIST SP 800-53, Revision 4 security controls. The goal of the Critical Controls is to strengthen the defensive posture of DOL's information security; reduce compromises, recovery efforts, and associated costs; and protect critical assets and infrastructure. The Controls provide continuous, automated monitoring of the most at-risk portions of DOL's IT infrastructure. Having them in place allows DOL to focus on its primary mission.

We held team discussions to consider possible fraud risk factors at DOL and its agencies. A fraud inquiry with DOL and agency management was conducted to consider fraud risk factors.

Testing

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

- Asking information system owners, Information Systems Security Officer (ISSO), system administrators and other relevant individuals to walk through each control

process.
- Inspecting the information security practices and policies established by the OCIO.
- Inspecting the information security practices, policies, and procedures in use across DOL.

As needed, we selected information systems to evaluate specific control elements related to of user account forms, terminated users, and configuration management changes.

We tested data reliability by obtaining system-generated lists and evaluating source documentation provided to support system-generated data. We compared source documentation to system-generated lists to determine the accuracy of that data.

Reporting

After completing system testing, we reported results to the agency official for the systems reviewed based on the testing of security controls. The results from testing of the financial systems were also used.

In planning and performing our work, we considered DOL's internal controls that were relevant to our objectives by obtaining an understanding of those controls and by assessing control risk for the purposes of achieving our objectives. Our objective was not to provide assurance on the internal controls. Therefore, we did not express an opinion on the internal controls as a whole. Our consideration of DOL's internal controls relevant to our objectives would not necessarily disclose all matters that might be reportable conditions. Because of the inherent limitations on internal controls, noncompliance may nevertheless occur and not be detected.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Quality Standards for Inspection and Evaluation. Those standards require that we plan and perform our work to obtain sufficient, appropriate evidence to provide a reasonable basis for our results and conclusions based on our evaluation objective. We believe that the evidence obtained provides a reasonable basis for our results and conclusions based on our objective.

CRITERIA

Our FISMA evaluation approach focused 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.

We used the following criteria in the performance of our evaluation:

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- FISMA of 2002
- FISMA revised 2014
- NIST SP 800-53 Revision 4

- Relevant NIST SP 800 documents
- Department of Labor Manual Series 9 - Information Management
- DOL Computer Security Handbook

APPENDIX II – ACRONYMS AND ABBREVIATIONS

ACRONYM	**DEFINITION**
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
DHS	Department of Homeland Security
DOL	Department of Labor
DOLCSIRC	DOL Computer Security Incident Response Capability
ETA	Employment and Training Administration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
IG	Inspector General
ISSO	Information Systems Security Officer
IT	Information Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OWCP	Office of Workers' Compensation Programs
PII	Personally Identifiable Information
POA&M	Plan of Action & Milestones
Q	Quarter
RTO	Recovery Time Objective
SP	Special Publication
US-CERT	United State Computer Emergency Readiness Team