U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE CHIEF INFORMATION OFFICER

FY 2017 FISMA DOL INFORMATION SECURITY REPORT

This report was prepared by KPMG LLP, under contract to the U.S. Department of Labor, Office of Inspector General, and by acceptance it becomes a report of the Office of Inspector General.

Elliot P. Lewis

Assistant Inspector General for Audit
U.S. Department of Labor

Date Issued:	December 29, 2017
Report Number:	23-18-001-07-725

U.S. Department of Labor

Office of Inspector General
Washington, DC. 20210

December 29, 2017

MEMORANDUM FOR: GUNDEEP AHLUWALIA
Chief Information Officer

Elliot P. Lewis

FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: FY 2017 FISMA DOL Information Security Report,
Report Number: 23-18-001-07-725

Attached is the Independent Auditors' Report on the U.S. Department of Labor's (DOL) Fiscal Year (FY) 2017 information security program and practices.

We contracted with KPMG LLP (KPMG) to conduct this independent evaluation. DOL's Office of Inspector General monitored KPMG's work to ensure it met professional standards and contractual requirements. KPMG conducted the individual evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants standards.

KPMG is responsible for the attached auditors' evaluation and the conclusions expressed in the report. In connection with the contracted work, we monitored their work and progress and 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, 2016, to September 30, 2017, to include DOL's compliance with Federal Information Security Management Act (FISMA) and related information security policies, procedures, standards, and guidelines. The determinations were based, in part, on a selection of DOL-wide security controls and a selection of system-specific security controls across 20 information systems. Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope, & Methodology*.

RESULTS

KPMG reported 33 findings in four security control areas, encompassing identity and access management, incident response, contingency planning, and configuration management. These findings included weaknesses not mitigated as a result of vulnerability scans; patches and performance monitoring tools not implemented; issues with separation of duties; improper monitoring of contractor onboarding and separation; account recertification not performed completely and accurately; incidents not reported timely; incident response technologies undefined; contingency testing not performed and separated user accounts not removed timely.

Consequently, KPMG determined DOL's information security program was not effective for FY 2017.

MOST NOTABLE CONCERN

In reviewing the FY 2017 results, we noted that DOL again had not been effectively removing access of separated users. We have been reporting on this recurring issue since 2007. Nine of fifteen systems tested this year still had active user accounts after individuals' employment had been terminated. One of these systems contained user accounts that appeared to have been accessed after the users' employment had been terminated.

Failing to promptly remove a separated user's account increases risk of harm to DOL's information systems. A disgruntled, separated user could wreak havoc by deleting files, compromising protected information, or corrupting the integrity of data.

We previously reported the following audit findings related to separated users:

> **2007 –** Two DOL information systems contained active user accounts for employees that were terminated. In one system, nine terminated users maintained active accounts and in the other system one terminated employee still had end-user access.
>
> **2008 –** Four DOL information systems contained active user accounts for employees that were separated from DOL. Specifically, three of the four information systems separated users that that accessed the system subsequent to separation.
>
> **2009 –** 17 DOL information systems contained a total of 93 terminated user accounts not disabled or deleted within the required time period, and 42 were still active at the time of the audit.

2010 – 11 DOL information systems contained user accounts that were not removed in a timely manner after the employee had separated. In five of those systems, accounts were active after user separation. For four of these five, former employees accessed their user accounts subsequent to their separation dates.

2011 – Nine DOL information systems contained a total of 95 separated employees retained access to network accounts after their departure.

2012 – 562 separated DOL employees held active PIV-II accounts after separation.

2013 – One DOL information system contained 37 terminated DOL employees' user accounts that retained access to the system for periods ranging from 3 to 407 days after their DOL HR termination dates.

2014 –10 DOL information systems and one data center contained accounts still active after individuals' separation dates, including four major information systems that had user accounts accessed after those users were separated.

2015 – Ten DOL information systems had active user accounts for terminated users and four of those systems had user accounts accessed after the users had been terminated.

2016 – Eight DOL information systems had user accounts for terminated individuals that were not removed timely and were not deactivated after a period of inactivity. Additionally, three user accounts were accessed after the termination date of the user.

CONTACT

Should you have any questions, please contact Stephen Fowler, Audit Director, at (202) 693-7013.

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 2017 Independent Evaluation of the U.S. Department of Labor's Federal Information Security Modernization Act of 2014 Management Systems Report

December 6, 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

BACKGROUND 3

Federal Information Security Modernization Act 3

FY 2017 Inspector General FISMA Reporting Metrics 3

OVERALL EVALUATION RESULTS 5

FINDINGS 7

Protect Function – Configuration Management 7

Protect Function – Identity and Access Management 10

Respond Function – Incident Response 14

Recover Function – Contingency Planning 15

MANAGEMENT RESPONSE TO THE REPORT 19

Appendices

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY 23

APPENDIX II – GLOSSARY 26

KPMG LLP
1676 International Drive
McLean, VA 22102

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

Re: Fiscal Year 2017 the U.S. Department of Labor's Federal Information Security Modernization Act Management Systems Report

This report presents the results of our independent evaluation of the U.S. Department of Labor's (DOL) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including DOL, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS has prepared the FISMA 2017 questionnaire to collect these responses. FISMA requires that the agency Inspectors General (IG) or an independent external auditor perform the independent evaluation as determined by the IG. DOL contracted with KPMG LLP (KPMG) to conduct this independent evaluation.

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

The objective for this independent evaluation was to determine if DOL implemented an effective FISMA information security program and practices for the period October 1, 2016 to September 30, 2017 for its information systems, including the DOL's compliance with FISMA and related information security policies, procedures, standards, and guidelines. We assisted the DOL Office of Inspector General (OIG) in categorizing the identified findings for the CyberScope metrics. We based our work, in part, on a selection of DOL-wide security controls and a selection of system-specific security controls across 20 information systems (15 DOL information systems, and 5 DOL contractor systems). Additional details regarding the scope of our independent evaluation are included in Appendix I, *Objective, Scope, Methodology and Criteria*.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, DOL established and maintained its information security program and practices for its information systems for the 5 cybersecurity functions[1] and 7 FISMA metric domains.[2] While the security program has been implemented across DOL, we identified 33 findings within 3 of the 5 cybersecurity functions and within 4 of the 7 FISMA metric domains, as follows:

- Protect – Configuration Management
- Protect – Identity and Access Management
- Respond – Incident Response
- Recover – Contingency Planning

[1] OMB, DHS, and CIGIE developed the FY 2017 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officers (CIO) Council. In FY 2017 the 7 IG FISMA metric domains were aligned with the 5 cybersecurity functions of identify, protect, detect, respond, and recover as defined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*.

[2] As described in the DHS' *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0,* the 7 FISMA metric domains are: risk management, configuration management, identity and access management, security training, information security continuous monitoring, incident response, and contingency planning.

We have made recommendations related to these control findings and additional program recommendations to the Chief Information Officer (CIO) that, if effectively addressed by management, should strengthen the respective information systems and DOL's information security program. In a written response, DOL CIO concurred with our findings and recommendations (see *Management Response*).

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

Sincerely,

KPMG LLP

December 6, 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 OMB, agency security policy, and risk-based standards and guidelines published by NIST related to information security practices.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, the Comptroller General of the United States, and selected congressional committees on the adequacy and effectiveness of agency information security policies and procedures. OMB has delegated some responsibility to DHS in memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, for the operational aspects of federal cybersecurity, such as establishing government-wide incident response and operating the tool to collect FISMA metrics. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

FY 2017 Inspector General FISMA Reporting Metrics

For Fiscal Year (FY) 2017, OMB, DHS, and CIGIE implemented changes to the IG FISMA reporting metrics to organize them around the 5 information security functions outlined in the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework):* identify, protect, detect, respond, and recover. In addition, CIGIE implemented maturity models for the FY 2017 FISMA metric domains: risk management (RM), configuration management (CM), identity and access management (IA), security training (ST), and contingency planning (CP), and revised the information security continuous monitoring (ISCM) and incident response (IR) maturity models that were instituted in FY 2015 and FY 2016, respectively.

In the past, the ISCM and IR models had maturity levels for people, process, and technology. In FY 2017, CIGIE eliminated specific people, process, and technology elements and, instead, issued specific questions. These models have 5 levels: ad-hoc, defined, consistently implemented, managed and measurable, and optimized. The introduction of a 5-level maturity model is a deviation from previous DHS guidance over the CyberScope questions.

OVERALL EVALUATION RESULTS

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, DOL's information security program and practices for its information systems were established and have been maintained for the 5 cybersecurity functions and 7 FISMA metric domains. The FISMA program areas are outlined in the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0* and were prepared by DHS' Office of Cybersecurity and Communications Federal Network Resilience. The CyberScope functions and domains are:

Function	Domain
Identify	Risk management
Protect	Configuration management, Identity and access management, and Security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

While a security program has been implemented across DOL, we identified 33 findings that we reported to DOL management in 3 of 5 FISMA metric functions. We have made recommendations related to these findings that, if effectively addressed by management, should strengthen the respective information systems and DOL's information security program. DOL has been implementing corrective actions, but they were not fully implemented and will be evaluated in FY 2018. 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.

We specifically noted the following findings in the 3 cybersecurity functions:

Cybersecurity Function: Protect

Domain: Configuration Management

- Vulnerability and configuration scans identified weaknesses, of various risk levels, that were not remediated or mitigated.
- Patches that correct security weaknesses were not implemented
- Tools to monitor performance of servers were not implemented.

Domain: Identity and Access Management

- Terminated accounts were not removed in a timely manner.
- A process to monitor onboarding and separation of all contractors was not identified.
- Account re-certifications for systems had not been performed completely and accurately for either privileged or non-privileged user accounts
- Separation of duties and a formally authorized waiver accepting risk posed by the separation of duties conflict was not identified.
- Separation of duties was not enforced during the review of operating system and database audit logs.
- Application level audit logging capabilities for systems were not appropriately configured.

Cybersecurity Function: Respond

- DOL did not report incidents timely and has not fully defined incident response technologies. (Domain: Incident Response)

Cybersecurity Function: Recover

- DOL did not perform failover and failback contingency testing for applications hosted on the general network environment. (Domain: Contingency Planning)
- The Business Impact Analyses (BIA) was not updated since March 2014. (Domain: Contingency Planning)
- Lessons learned from the most recent testing of the contingency planning have not been documented or implemented into the contingency plan for an application. (Domain: Contingency Planning)

The *Findings* section of this report presents the detailed findings and associated recommendations that were communicated to the system owners and additional program recommendations for the CIO. In a written response to this report, the DOL CIO concurred 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.

FINDINGS

1. Protect Function – Configuration Management

Vulnerability and configuration scans identified weaknesses, of various risk levels, that were not remediated or mitigated.

Vulnerability and configuration scans were performed on a selection of financial systems. Weaknesses were identified that were not remediated or mitigated in accordance with the DOL's defined timelines. Specifically, a total of 263 weaknesses (182 configuration management, and 81 patch management) of various risk levels (17 critical, 40 high, and 206 medium) were identified.

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

Volume 14 of the DOL Computer Security Handbook (CSH) stated that:
1. DOL agencies must:

a. Scan for vulnerabilities in the information system and hosted applications at least annually and when new vulnerabilities potentially affecting the system / applications are identified and reported.

b. Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations
- Formatting and making transparent, checklists and test procedures
- Measuring vulnerability impact.

c. Analyze vulnerability scan reports and results from security control assessments.

d. Remediate legitimate vulnerabilities according to an agency assessment of risk and system vulnerability (recommended high risks immediately but no later than three months from discovery and moderate risks within six months) in accordance with an organizational assessment of risk.

e. Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the Department to help eliminate similar vulnerabilities in other information systems (i.e. systemic weaknesses or deficiencies).

2. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (including but not limited to, vulnerability scanning tools for applications, source code reviews, and/or static analysis of source code).

3. Agencies must, at a minimum, implement network-based active vulnerability scanning. Agencies are highly encouraged to implement host-based active vulnerability scanning to further identify and correct system vulnerabilities.

Patches that correct security weaknesses were not implemented.

For five of fifteen systems tested, DOL did not consistently follow policies and procedures identified in the CSH for implementing patches that correct security weaknesses.

Strong Configuration Management control practices are intended to reduce the risk of system exposure to known findings, malicious technical attacks, and unauthorized or unintentional changes. By not appropriately patching the network to correct security weakness, DOL systems hosted on the network are at risk.

> Volume 17 of the DOL CSH states Office of the Chief Information Officer (OCIO) security reserves the right to specify a minimum level of importance (including, but not limited to, minimum requirements) for updates that have been released by approved sources. In instances where OCIO Security does not specify minimum requirements for updates, information system personnel shall develop, implement, and comply with any and all agency requirements. The minimum requirements for installing updates on information systems are as follows:
>
> a. Updates identified as critical importance (including all out of cycle updates) must be installed within 72 hours of release.
> b. Updates identified as high importance must be installed within five (5) business days of release.
> c. Updates identified as moderate importance must be installed within 10 business days of release.
> Updates identified as low importance must be installed within 20 business days of release.

Tools to monitor performance of servers were not implemented.

A DOL system, did not have SolarWinds, Nagios, or any other tool implemented to monitor the performance of servers that support the application and database.

Without system performance monitoring and real-time alerts, Office of the Assistant Secretary for Administration and Management (OASAM) personnel are unable to receive timely notification of a critical server going down. In an event like this, the server may not be able to be brought back online in a timely manner, leading to a loss of the availability and integrity of data in the application and database.

Volume 17 of the DOL CSH states that:

> DOL's additional required minimum standards on monitoring information systems for Moderate and High information systems are as follows:
>
> 1. The agency employs automated tools to support near real-time analysis of events.
>
>   [...]
>
> 3. The information system alerts agency and/or enterprise designated individuals when agency-defined indications of compromise or potential compromise occur (such as irregular consumption or audit function disablement).

We have made the following recommendations to the system owners:

1. Prioritize and enforce patching of operating systems and databases timely in accordance with the patching criticality timeframes that are documented in DOL CSH policies and procedures;
2. Provide training to relevant personnel on the patch management process (timing, approval, testing, implementation, and documentation); and
3. Document a Policy/Procedure Exemption Risk Management Request Form for the patching of relevant application servers, and submit it to the OCIO for review and authorization.
4. Continue to implement SolarWinds for full system monitoring functionality. In the meantime, we recommend that OASAM personnel continue to utilize Nagios to perform system performance monitoring functions until SolarWinds is fully implemented.

2. Protect Function – Identity and Access Management

Terminated accounts were not removed in a timely manner.

Nine of fifteen systems tested still had active user accounts after individuals' employment had been terminated. One of these systems contained user accounts that appeared to have been accessed after those users' employment had been terminated, ranging from 4 to 266 days after their termination.

Removing access when user accounts are terminated reduces the risk of unauthorized access. Accounts for these users were either currently active as of testing or had been active after the users' termination dates.

> Volume 13 of the DOL CSH states:
>
> When employment is terminated, the agency shall:
>
> 1. Disable information system access within the 24 hours of that employee's separation when termination is voluntary.
> 2. 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)

A process to monitor onboarding and separation of all contractors was not identified.

DOL does not have an entity-wide process to monitor the separation of all contractors that support DOL programs. Failure to maintain and monitor a complete and accurate listing of contractor separation data impairs DOL's ability to remove separated contractor's access timely and increases the likelihood of unauthorized access to financial systems.

> Volume 13 of the DOL CSH states:
>
> When employment is terminated, the agency shall:
>
> 3. Disable information system access within the 24 hours of that employee's separation when termination is voluntary.
> 4. 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)

Account re-certifications for systems had not been performed completely and accurately for either privileged or non-privileged user accounts.

Seven of fifteen systems tested had not performed complete and accurate periodic account re-certifications for either privileged or non-privileged user accounts on at least an annual basis per DOL policy.

> Volume 1 of the DOL CSH states that information system accounts (agency determined sample based on assessment of risk) must be reviewed every 6 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.

Without the implementation of a proper account recertification process there is an increased possibility that a user may inappropriately retain access to system applications. Additionally, users with incompatible or unnecessary roles could maintain these privileges without management awareness of the issue. Left unmonitored, this could lead to violations of the concept of least privilege or lead to information system account compromises.

Separation of duties and a formally authorized waiver accepting risk posed by the separation of duties conflict was not identified.

An application lacked appropriate separation of duties and a formally authorized waiver accepting the risk posed by the separation of duties conflict.

> Volume 1 of the DOL CSH states that DOL's required minimum standards on enforcing separation of duties for Moderate and High information systems are as follows:
>
> 1. Separate duties of general and privileged users as necessary, to prevent malevolent activity without collusion.
> 2. Document separation of duties of individuals.
> 3. Define information system access authorizations to support separation of duties.

Failure to periodically review the risks posed by allowing accounts to have privileged access to both the database and the operating system could expose the agency to risks that have not been identified since the last review or that are no longer acceptable to the agency. Specifically, by not enforcing separation of duties, an individual with a combination of database administrator access and system administrator access could complete unauthorized transactions, hide unauthorized activity, and/or override controls.

Separation of duties was not enforced during the review of operating system and database audit logs.

Of the systems tested, six of fifteen had Audit Logging and Accountability control findings. The systems' audit log reviews are performed by users who perform security functions on the operating system and database servers, which leads to a separation of duties conflict.

> Volume 1 of the DOL CSH states:
> "Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties may include but not exclusive to the following examples:
> 1. Dividing mission functions and information system support functions among different individuals and/or roles;
> 2. Conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security);
> 3. Ensuring security personnel administering access control functions do not also administrator audit functions; and
> 4. Different administrator accounts exist and are used for different roles"

Application level audit logging capabilities for systems were not appropriately configured.

Four of fifteen systems tested did not completely and accurately monitor and review all of their application auditable events.

> Volume 3 of DOL's CSH states that DOL's required minimum standards on managing information system audit events are as follows:
> 1. Determine, based on a risk assessment and mission/business needs, that the information system is capable of auditing the following events:
>   a. Account creation, modification, disabling, and deletion;
>   b. Administrative permissions executed on user accounts (including but, not limited to, inclusion in access groups, reset of password, account lockout override);
>   c. Administrative permissions executed on a system resource (including, but not limited to, addition of users or groups to access lists, creation of share points, creation of new access groups, change of access group permissions);
>   d. Failed login attempts and account lock;
>   e. Use of 'su', 'pu', 'root', and 'administrator', or equivalent accounts;
>   f. Activity log roll-over, deletion, or editing; and
>   g. All computer-readable data extracts from databases containing personally identifiable information (PII).
> 2. 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.

Without documenting complete and accurate audit logs systems were at an increased level of risk of fraudulent activities that might compromise data. Without proper and timely review of audit logs, unauthorized access or activity could not be identified in any of the systems.

We have made the following recommendations to the system owners:

1. Develop and implement additional controls to ensure that separated users are deactivated timely from DOL in accordance with the DOL CSH;
2. Employ an automated mechanism to deactivate all application accounts connected to the lightweight directory access protocol (LDAP) when the network account is removed, if feasible;
3. Implement an audit logging solution to capture application users' account actions in accordance with the CSH;
4. Implement separation of duties principles between the reviewer of audit logs and the administrators performing security functions on the operating system, database and application hosts;
5. Provide training, promulgate and enforce the audit logging process and policies and procedures to ensure that all relevant personnel are aware of the process requirements;
6. Enforce access recertification policies and procedures to ensure that all users with network access, including those with access to migrate source code to production, are reviewed every six months for appropriateness of permissions granted;
7. Complete and document the recertification of the users with access to develop and migrate source code to systems for the appropriateness of permissions granted.

3. Respond Function – Incident Response

DOL did not report incidents timely and has not fully defined incident response technologies.

Incidents from the network were not reported from the DOL Computer Security Incident Response Capability (DOLCSIRC) team to the US-Computer Emergency Readiness Team (US-CERT) within one hour. Also, DOL has not fully identified and defined requirements for incident response technologies regarding web application firewalls, intrusion detection systems, and file integrity tools.

> Volume 8 of the DOL CSH states that DOL's required minimum standards on incident reporting are as follows:
>
> 1. DOLCSIRC shall report the incident to OIG, US-CERT, Office of Public Affairs (OPA), the DOL Physical Security Officer, and DOL Senior Management (including but not limited to Deputy Secretary, CIO), as appropriate.
> 2. Incident reports must be submitted to DOLCSIRC via e-mail to dolcsirc@dol.gov. Confirmed Incidents need to be reported within One Hour upon discovery. Suspected 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 are required to submit a DOLCSIRC incident reports form following the verbal notification.

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

We have made the following recommendations to the system owners:

1. Periodically conduct training to review the Incident Management Standard Operating Procedure and incident response reporting guidelines with all agencies;
2. Implement the appropriate incident response technologies based upon defined requirements and applicable policy; and
3. Update the Incident Response Plan to reflect updated technologies and provide training to relevant personnel groups.

4. Recover Function – Contingency Planning

DOL did not perform failover and failback contingency testing for applications hosted on the general network environment.

The general network environment provides the overall support system for non-applicant support such as back-ups. A lack of coordination among agencies Information Security Officers and OASAM (the hosting organization) for contingency planning activities resulted in failover and failback testing not being performed.

> Volume 6 of the DOL CSH states the following policy, procedures, and standards must be implemented for all Low, Moderate, and High information systems:
>
> 1. DOL agencies perform tests of the contingency plan for the information system to determine the effectiveness of the plan, and the organizational readiness to execute the plan, reviews the contingency plan test results, and initiates corrective actions, if needed
> 2. A full failover test to a hot/warm/cold site must be performed periodically (e.g. annually or bi-annually) if the site is identified as a part of the contingency plan.
> 3. The contingency plan must be tested at least annually using agency-defined tests and exercises to determine the plan's effectiveness and the agency's readiness to execute the plan.
>
> DOL's additional required minimum standard on developing a contingency plan for Moderate and High information systems is as follows:
>
> 1. The contingency plan development must be coordinated with agency elements responsible for related plans (including but not limited to, Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Cyber Incident Response Plan, Crisis Communications Plan, Critical Infrastructure Plan, Insider Threat Implementation Plan, and Occupant Emergency Plan).

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

The Business Impact Analyses has not been conducted for a system since March, 2014.

The BIA for an application has not been updated in over three years due to a major system update.

> Volume 6 of the DOL CSH states that DOL's required minimum standards on developing a contingency plan are as follows:
>
> > A contingency plan must be developed and implemented for DOL information systems. The contingency plan and supporting IT Business Impact Assessment (BIA):
> >
> > 1. Identifies essential missions and business functions and associated contingency requirements.
> > 2. Provides recovery objective, restoration priorities, and metrics.
> > 3. Addresses contingency roles, responsibilities, assigned individuals with contact information.
> > 4. Addresses maintaining essential business functions despite an information system disruption, compromise, or failure.
> > 5. Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented and
> > 6. Is reviewed and approved by designated officials within the agency.

Without the continual testing of a BIA over the application, there is an increased risk of contingency plan testing not addressing relevant threats or impacts to the confidentiality, integrity, and availability of data stored in the application.

Lessons learned from the most recent testing of the contingency planning have not been documented or implemented into the contingency plan for an application.

An application's test plan did not contain any lessons learned from the most recent test due to an oversight by management in updating the current contingency plan and test results.

> Volume 6 of the DOL CSH states that DOL's required minimum standards on contingency plan testing are as follows:
>
> 1. The contingency plan must be tested at least annually using agency-defined tests and exercises to determine the plan's effectiveness and the agency's readiness to execute the plan.

2. The Agency tests and/or exercises the contingency plan for the information system at least annually for Moderate and High impact systems and at least every three years for Low impact systems. At a minimum, functional exercises must be conducted for Moderate and High impact systems and classroom / tabletop exercises for Low impact systems to determine the plan's effectiveness and the agency's readiness to execute the plan.
3. The Agency reviews the contingency plan test/exercise results and initiates corrective actions.
4. The results of contingency plan testing must be used to identify and remediate potential weaknesses.
5. The appropriate personnel shall review the contingency plan tests results, which must be documented in the contingency plan, and initiate corrective actions.
6. The agency coordinates contingency plan testing and/or exercises with Departmental elements responsible for related plans for Moderate and High systems.

Without the implementation of a Contingency Plan Test that addresses failover, failback, server clustering, and disk mirroring, there is an increased risk of loss of data from the application system. Additionally, the absence of a fully developed and documented Contingency Plan, periodic testing of the plan, and updating of the plan to include lessons learned will increase the risk of a compromise of the confidentiality, integrity, and availability of the data residing on the information system in the event of a disaster.

We have made the following recommendations to the system owners:

1. Implement an appropriate Contingency Plan/BIA planning and testing process per the requirements outlined in the DOL CSH, to include annual failover and failback tests for each system hosted on the network.

Recommendations to the Chief Information Officer

Although DOL had established an information security program and practices across the Agency, we identified numerous deficiencies that may limit the Agency's ability to protect adequately the organization's information, PII, and information systems. Specifically, management charged with oversight and accountability for the DOL information security program had not taken appropriate action to address these deficiencies that have been reported to them since FY 2003.

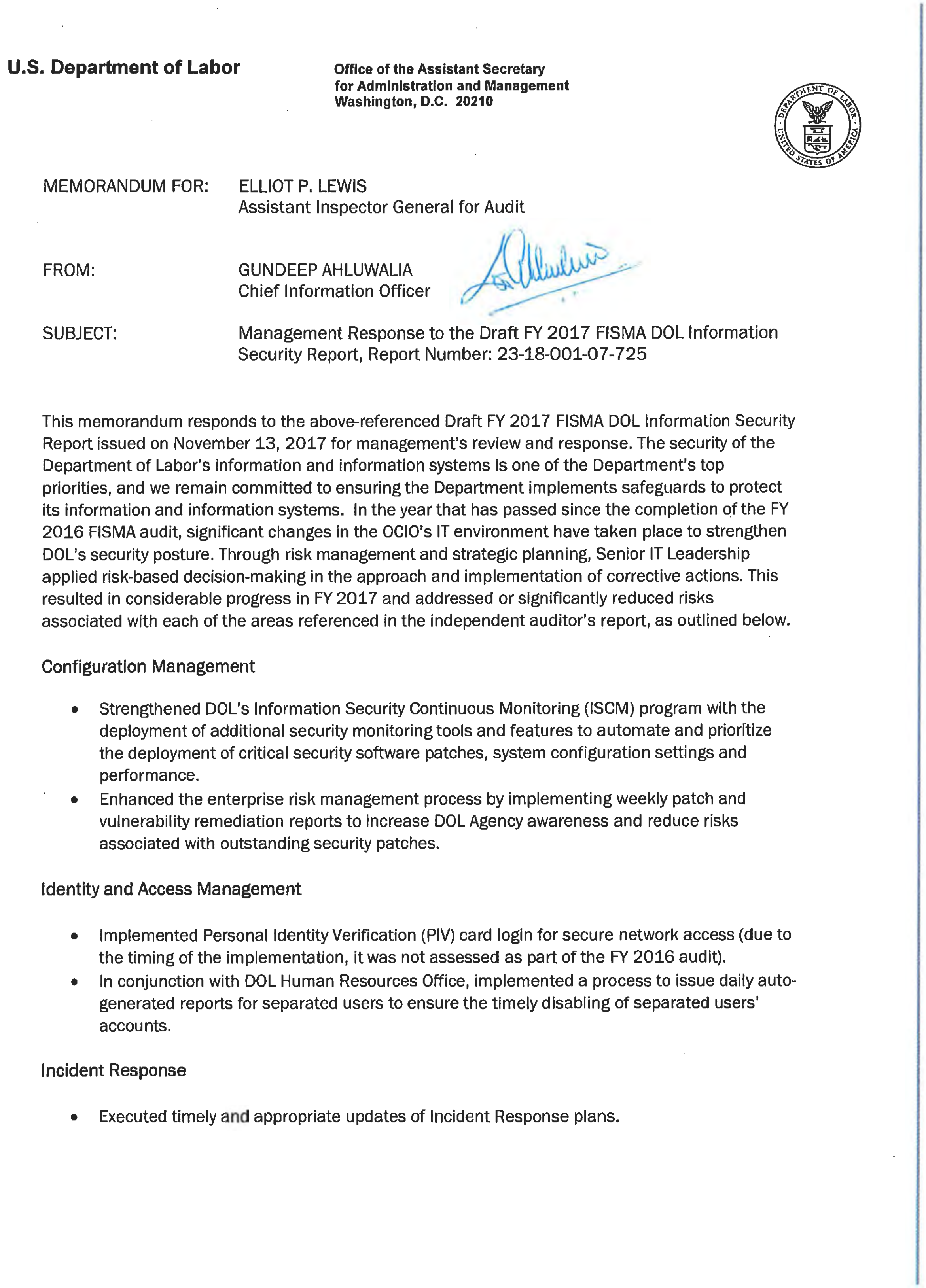
Without appropriate security, DOL may not be able to protect its mission assets adequately. As such the Agency's systems, and the sensitive data they contain, are at risk. Deficiencies we identified could negatively affect the confidentiality, integrity, and availability of the Agency's systems and PII. 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:

1. Conduct a sufficient risk assessment to identify the root causes of the identified deficiencies;
2. Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies that have been communicated to DOL management;
3. Coordinate efforts among the DOL agencies to design and implement procedures and controls to address account management, system access settings, configuration management, system audit log configuration and reviews, and patching and vulnerability management control deficiencies in key financial feeder systems; and
4. Monitor the agencies' progress to ensure that established procedures and controls are operating effectively and maintained.

MANAGEMENT RESPONSE TO THE REPORT

The following is DOL CIO's response, November 29, 2017, to the FY 2017 FISMA Evaluation Report.



U.S. Department of Labor

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

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

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

SUBJECT: Management Response to the Draft FY 2017 FISMA DOL Information Security Report, Report Number: 23-18-001-07-725

This memorandum responds to the above-referenced Draft FY 2017 FISMA DOL Information Security Report issued on November 13, 2017 for management's review and response. The security of the Department of Labor's information and information systems is one of the Department's top priorities, and we remain committed to ensuring the Department implements safeguards to protect its information and information systems. In the year that has passed since the completion of the FY 2016 FISMA audit, significant changes in the OCIO's IT environment have taken place to strengthen DOL's security posture. Through risk management and strategic planning, Senior IT Leadership applied risk-based decision-making in the approach and implementation of corrective actions. This resulted in considerable progress in FY 2017 and addressed or significantly reduced risks associated with each of the areas referenced in the independent auditor's report, as outlined below.

Configuration Management

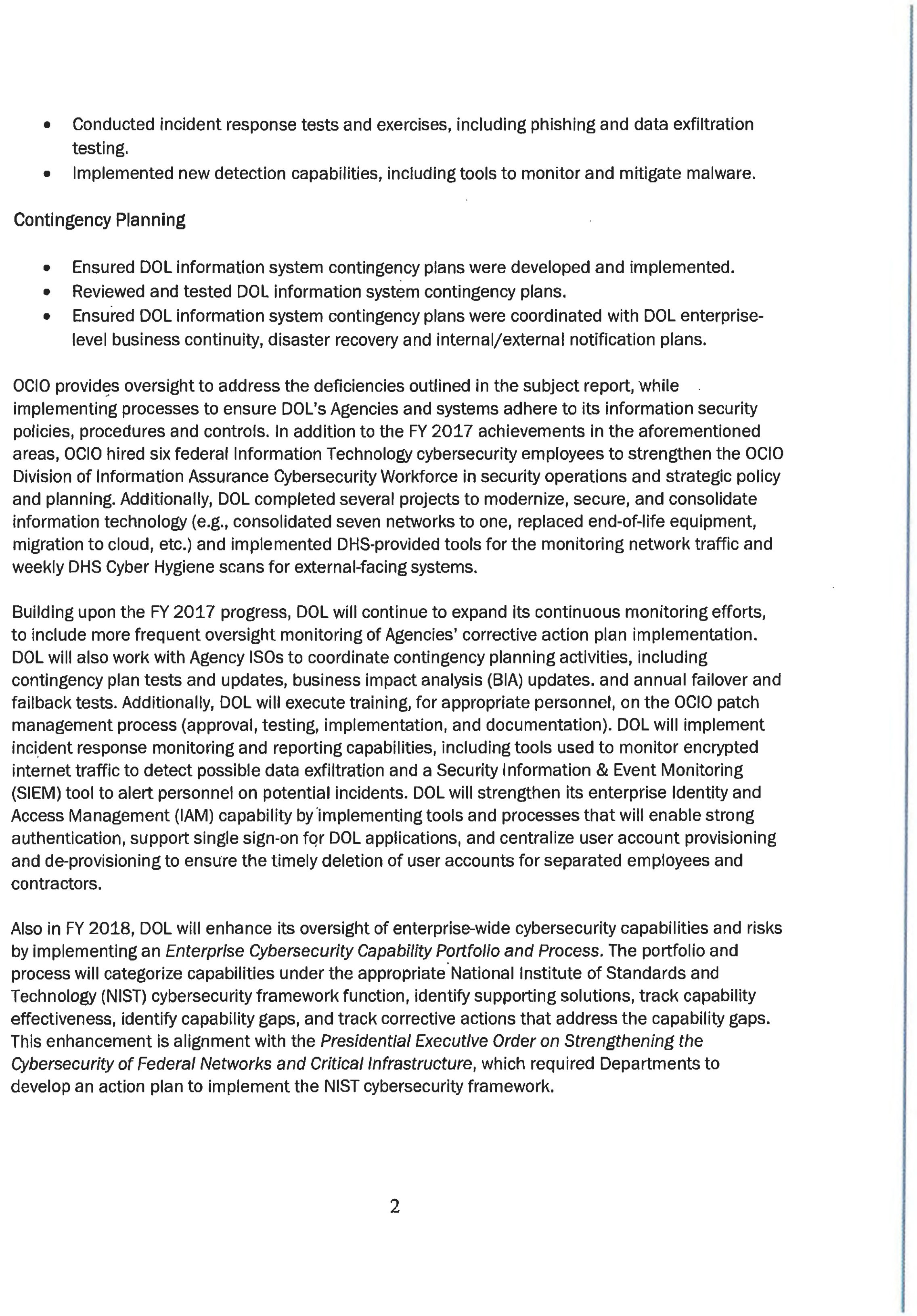
- Strengthened DOL's Information Security Continuous Monitoring (ISCM) program with the deployment of additional security monitoring tools and features to automate and prioritize the deployment of critical security software patches, system configuration settings and performance.
- Enhanced the enterprise risk management process by implementing weekly patch and vulnerability remediation reports to increase DOL Agency awareness and reduce risks associated with outstanding security patches.

Identity and Access Management

- Implemented Personal Identity Verification (PIV) card login for secure network access (due to the timing of the implementation, it was not assessed as part of the FY 2016 audit).
- In conjunction with DOL Human Resources Office, implemented a process to issue daily auto-generated reports for separated users to ensure the timely disabling of separated users' accounts.

Incident Response

- Executed timely and appropriate updates of Incident Response plans.



- Conducted incident response tests and exercises, including phishing and data exfiltration testing.
- Implemented new detection capabilities, including tools to monitor and mitigate malware.

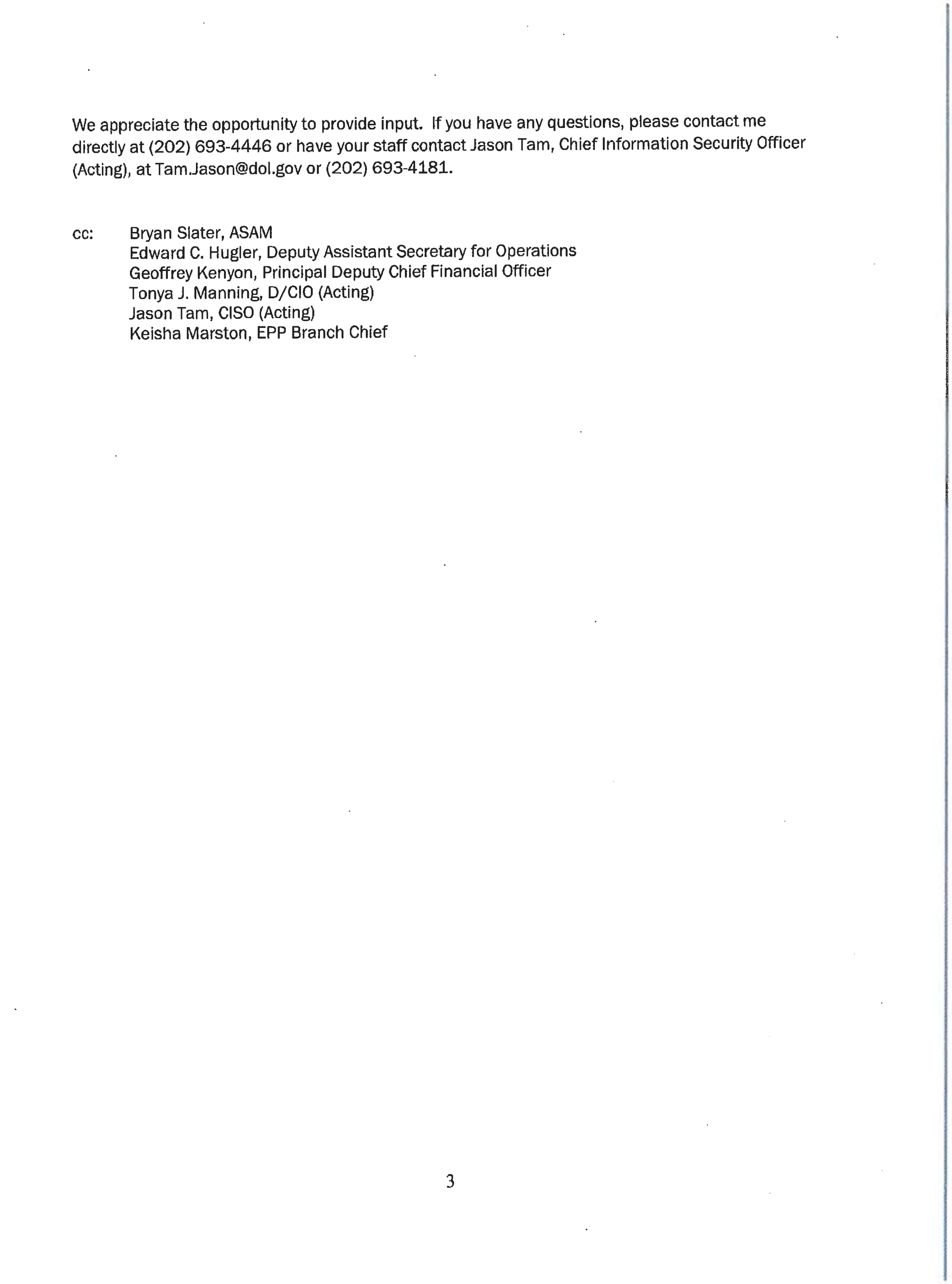
Contingency Planning

- Ensured DOL information system contingency plans were developed and implemented.
- Reviewed and tested DOL information system contingency plans.
- Ensured DOL information system contingency plans were coordinated with DOL enterprise-level business continuity, disaster recovery and internal/external notification plans.

OCIO provides oversight to address the deficiencies outlined in the subject report, while implementing processes to ensure DOL's Agencies and systems adhere to its information security policies, procedures and controls. In addition to the FY 2017 achievements in the aforementioned areas, OCIO hired six federal Information Technology cybersecurity employees to strengthen the OCIO Division of Information Assurance Cybersecurity Workforce in security operations and strategic policy and planning. Additionally, DOL completed several projects to modernize, secure, and consolidate information technology (e.g., consolidated seven networks to one, replaced end-of-life equipment, migration to cloud, etc.) and implemented DHS-provided tools for the monitoring network traffic and weekly DHS Cyber Hygiene scans for external-facing systems.

Building upon the FY 2017 progress, DOL will continue to expand its continuous monitoring efforts, to include more frequent oversight monitoring of Agencies' corrective action plan implementation. DOL will also work with Agency ISOs to coordinate contingency planning activities, including contingency plan tests and updates, business impact analysis (BIA) updates. and annual failover and failback tests. Additionally, DOL will execute training, for appropriate personnel, on the OCIO patch management process (approval, testing, implementation, and documentation). DOL will implement incident response monitoring and reporting capabilities, including tools used to monitor encrypted internet traffic to detect possible data exfiltration and a Security Information & Event Monitoring (SIEM) tool to alert personnel on potential incidents. DOL will strengthen its enterprise Identity and Access Management (IAM) capability by implementing tools and processes that will enable strong authentication, support single sign-on for DOL applications, and centralize user account provisioning and de-provisioning to ensure the timely deletion of user accounts for separated employees and contractors.

Also in FY 2018, DOL will enhance its oversight of enterprise-wide cybersecurity capabilities and risks by implementing an *Enterprise Cybersecurity Capability Portfolio and Process.* The portfolio and process will categorize capabilities under the appropriate National Institute of Standards and Technology (NIST) cybersecurity framework function, identify supporting solutions, track capability effectiveness, identify capability gaps, and track corrective actions that address the capability gaps. This enhancement is alignment with the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which required Departments to develop an action plan to implement the NIST cybersecurity framework.



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

cc: Bryan Slater, ASAM
Edward C. Hugler, Deputy Assistant Secretary for Operations
Geoffrey Kenyon, Principal Deputy Chief Financial Officer
Tonya J. Manning, D/CIO (Acting)
Jason Tam, CISO (Acting)
Keisha Marston, EPP Branch Chief

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

Did DOL implement effective FISMA minimum information security requirements?

SCOPE

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation, Presidential directives, and the DHS *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0,* dated April 17, 2017. 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.

We made a selection of 20 information systems (15 DOL and 5 DOL contractor information systems) from a total population of 55 major applications and general support systems (GSS) as of January 27, 2017. Our testing also include DOL wide information security controls.

METHODOLOGY

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

- Inquired of information system owners, system administrators and other relevant individuals to walk through each control process.
- Inspected the information security practices and policies established by the OCIO.
- Inspected the information security practices, policies, and procedures in use across DOL.
- Inspected the artifacts to determine the implementation and operating effectiveness of security controls.

We performed our fieldwork at DOL's headquarters offices in Washington, District of Columbia (D.C.) during the period of April 4, 2017 through September 30, 2017. During our evaluation, we met with DOL management to provide a status of the engagement and discuss our preliminary conclusions.

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

<u>Criteria</u>

We focused our FISMA evaluation approach on federal information security guidance developed by NIST and OMB. NIST Special Publications provide guidelines that are considered essential to the development and implementation of agencies' security programs. The following is a listing of the criteria used in the performance of the FY 2017 FISMA evaluation:

NIST, Federal Information Processing Standard (FIPS) and/or Special Publications[3]

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
- NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*
- NIST Special Publication 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST Special Publication 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*
- NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- NIST Special Publication 800-60 Revision 1, Volume *I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- NIST Special Publication 800-61 Revision 2, *Computer Security Incident Handling Guide*
- NIST Special Publication 800-63-2, *Electronic Authentication Guideline*
- NIST Special Publication 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*

OMB Policy Directives

- OMB Circular A-130, *Managing Information as a Strategic Resource*
- M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*
- M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*
- OMB Memorandum 15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*

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

- M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- M-12-05, *Update on Contingency Planning*
- OMB Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*
- OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
- OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
- OMB Memorandum 06-16, *Protection of Sensitive Agency Information*
- OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*

United States Department of Homeland Security

- FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics V1.0 April 17, 2017

DOL Policy Directives

- DOL Computer Security Handbook Edition 5.0, Version 1.0 dated May 2014

APPENDIX IV – GLOSSARY

ACRONYM	DEFINITION
Act, the	Title III of the E-Government Act of 2002
AICPA	American Institute of Certified Public Accountants
BIA	Business Impact Analysis/Assessment
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Planning
CSH	Computer Security Handbook
Cybersecurity Framework	NIST Framework for Improving Critical Infrastructure Cybersecurity
D.C.	District of Columbia
DHS	Department of Homeland Security
DOL	U.S. Department of Labor
DOLCSIRC	DOL Computer Security Incident Response Capability
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
IA	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
KPMG	KPMG LLP
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
PII	Personally Identifiable Information
RM	Risk Management
ST	Security Training

ACRONYM	**DEFINITION**
US-CERT	United States Computer Emergency Readiness Team

TO REPORT FRAUD, WASTE, OR ABUSE

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

Telephone: 1-800-347-3756
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