APPENDIX B: AGENCY'S RESPONSE TO THE REPORT

U.S. Department of Labor

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

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

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

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

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

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

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

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

IT GOVERNANCE CONCERN

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

Management has taken action regarding each of the findings.

Finding	Status

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

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

CYBERSECURITY FUNCTION: IDENTIFY

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

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

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

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

CYBERSECURITY FUNCTION: PROTECT

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

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

CYBERSECURITY FUNCTION: RESPOND

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

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

CYBERSECURITY FUNCTION: RECOVER

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

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

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

RECOMMENDATIONS

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

OCIO will:

- Conduct a risk assessment to identify and document the root causes of the identified deficiencies;
- Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies in this report;
- Direct efforts to design and implement procedures and controls to address account management, system access settings, configuration management, system audit log configuration and reviews, and patching and vulnerability management control deficiencies in key financial feeder systems;

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

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

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