


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