U.S. Department of Labor

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

MEMORANDUM FOR: CAROLYN R. HANTZ
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA Digitally signed by GUNDEEP AHLUWALIA Date: 2022.01.05 17:38:14 -05'00'

SUBJECT: Management Response to the DRAFT REPORT - (Fiscal Year) *FY 2021 FISMA DOL Information Security Continuous Monitoring Controls Remain Deficient Report*, Report Number: 23-22-001-07-725

This memorandum responds to the above-referenced Draft Report – (Fiscal Year) *FY 2021 FISMA DOL Information Security Continuous Monitoring Controls Remain Deficient Report*, issued December 15, 2021. Cybersecurity continues to be a top priority at the Department, and DOL leadership remains committed to continuously strengthening DOL's cybersecurity posture. DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve upon within the cybersecurity program.

Management generally concurs with the findings identified during the FY 2021 FISMA audit evaluation and described in the draft report. In all cases, we have either since addressed the associated recommendations or have developed plans to address them in FY 2022. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).

During FY 2021, the Department took several actions to strengthen DOL's cybersecurity program, including in areas prioritized under Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021). For example, the Department developed a roadmap for Zero Trust, enhanced policy and procedure for Secure Supply Chain, and continued implementing enterprise-wide solutions to enhance encryption, multifactor authentication, IT asset management, incident response and incident monitoring. The Department continued deployment of additional Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) tools for vulnerability management, implementation of new Data Loss Prevention mechanisms, and transition of FISMA systems due for periodic reauthorization into Ongoing Authorization. Moreover, DOL provided additional risk-based security and privacy awareness trainings – including quarterly phishing exercises -- to address increased cybersecurity risks faced by remote users. In the areas of incident detection and response, DOL successfully deployed its Vulnerability Disclosure Program and enhanced its 24x7 Security Operations Center (SOC) to substantially reduce critical vulnerabilities within the Department.

DOL achieved the following positive cybersecurity results during FY 2021:

- Met all 10 of the President's Management Agenda (PMA) Cross-Agency Priority (CAP) Cybersecurity goals.
- Maintained the highest rating of "Managed Risk" across all measured function areas in the FY 2021 Risk Management Assessment (RMA) portion of the CIO FISMA report.
- Closed 12 previously open cyber-related OIG findings from previous years.
- Made the following improvements based on OIG recommendations:

  - Established a comprehensive inventory of web applications, developed a process, and distributed guidance to maintain the inventory centrally in order to better protect DOL's web applications from external threat.
  - Provided awareness training for multiple function areas, such as third-party continuous monitoring, identity and access management, and patch management.
  - Continued to improve POA&M oversight with updated procedures and reporting, providing leadership with a better view of cybersecurity risks.
  - Implemented SECURE Technology Act requirements to address organizational cyber supply chain risk.
  - Developed processes to ensure data backups are monitored for successful completion and that actions are taken timely to resolve data backup failures.
  - Improved PIV card processes by developing and implementing a system that maintains and tracks the employment status of DOL contractors with PIV cards and automatically notifying the appropriate stakeholders when contractors are separated to provide appropriate access control.
  - Developed and implemented a new enterprise-wide cybersecurity risk management strategy and program, aligned with NIST SP 800-39 and NIST SP 800-53, Rev. 4.
- Improved the FISMA OIG-determined maturity level in 6 of the 57 (11 percent) individual control areas compared to FY 2020, resulting in 20 of 57 (35 percent) areas rated as *Effective* (Level 4 or Level 5), including three areas rated at the highest level of *Optimized*.

Looking ahead, DOL will continue to focus on strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. The Department intends to:

- Continue to improve in the adoption of multifactor authentication and encryption of data-at-rest and in-transit;
- Reinforce and improve in the protection of critical software and mature capabilities for supply chain risk management;
- Continue efforts to transition DOL's network infrastructure to Internet Protocol Version 6;
- Continue its enhancement of DOL's information security continuous monitoring (ISCM) capability by implementing key performance indicators (KPIs) at the Enterprise-, Mission/Business Process-, and System-level, and implementing DHS' recently updated CDM agency-level dashboard; and
- Continue SOC enhancements that will allow the Department to anticipate and mitigate risk, and stay ahead of the evolving threat landscape.

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 (CISO), at Blahusch.Paul.E@dol.gov or (202) 693-1567. As the CISO, Paul Blahusch is the responsible party for the corrective actions identified in this correspondence.

cc: Rachana Desai Martin, Assistant Security for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Geoff Kenyon, Deputy Assistant Secretary for Budget and Performance
Paul Blahusch, Chief Information Security Officer
Karl Hellmann, Deputy Chief Information Security Officer
Muhammad Butt, Division Director, Information Security Policy & Planning (ISSP)