


**APPENDIX C: AGENCY'S RESPONSE TO THE REPORT**

<b>U.S. Department of Labor</b>	<b>Office of the Assistant Secretary for Administration and Management Washington, D.C. 20210</b>	
<b>MEMORANDUM FOR:</b>	CAROLYN RAMONA HANTZ Assistant Inspector General for Audit	
<b>FROM:</b>	LOUIS CHARLIER Acting Chief Information Officer	LOUIS CHARLIER Digitally signed by LOUIS CHARLIER Date: 2024.10.21 18:10:45 -0400
<b>SUBJECT:</b>	Management Response to DRAFT REPORT – (Fiscal Year) FY 2024 FISMA DOL Information Security Report: 23-25-002-07-725	
<p>This memorandum responds to the above-referenced <i>Draft Report – FY 2024 FISMA DOL Information Security Report: 23-25-002-07-725</i>, issued October 4, 2024. Information security continues to be a top priority at the Department, and DOL leadership remains committed to continuously strengthening DOL's information security posture. DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas to improve upon within the information security program and is actively working to address those areas.</p> <p>Management generally concurs with the findings identified during the FY 2024 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 2025. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).</p> <p>Although the result of the audit, following the Office of Management and Budget's guidance, determined that the Department of Labor's (DOL) information security program falls short of being effective, we firmly assert the contrary, backed by substantial evidence of our program's efficacy and continuous improvement. Our advancements in Information Security Continuous Monitoring (ISCM) and Vulnerability Management are testament to our unwavering efforts in fortifying our information security framework. The creation of tiered reports and the significant improvements in our vulnerability remediation process serve as strong proof of our forward momentum, offering both the quantitative and qualitative metrics of our effectiveness. It's noteworthy that 68% of the Inspector General's metrics were rated as Effective, underscoring our program's robustness. Furthermore, DOL's ability to resolve numerous recommendations from previous years showcases our proactive and diligent efforts in rectifying identified weaknesses.</p> <p>Our adoption of a risk-based strategy, in line with NIST recommendations and M-24-04 guidelines, highlights DOL's commitment to implementing a dynamic and resilient information security practice capable of adapting to the ever-changing threat landscape. This strategic approach not only addresses minor compliance discrepancies but also significantly contributes to the overarching success and effectiveness of our information security program.</p> <p>In Fiscal Year 2024, DOL made significant strides in enhancing its information security program, particularly in areas emphasized by Executive Order 14028, "Improving the Nation's Cybersecurity." Our ongoing initiatives to deploy enterprise-wide encryption for data-at-rest and in-transit, alongside the implementation of multifactor authentication, are pivotal to our cybersecurity framework. Our collaboration with the Department of Homeland Security in rolling out the Continuous Diagnostics and Mitigation (CDM) capability, coupled with our effective use of the Technology Modernization Fund to advance a zero-trust architecture, are critical milestones in meeting the Executive Order's mandates. Given these comprehensive enhancements and strategic initiatives, we stand by our</p>		

position that the DOL's information security program is not only effective but also exemplifies a model of continuous improvement and adaptability in the face of evolving cybersecurity challenges.

DOL accomplished the following additional information security results during FY 2024:

- During the FY 2024 FISMA Audit, DOL worked with OIG to close 18 prior year (PY) IT audit recommendations, reducing the number of open PY recommendations by more than 55 percent. Specifically, 4 of the recommendations closed were related to Vulnerability & Patch Management, which is a testament to DOL's enhanced vulnerability remediation procedures and in support of the DHS DOL CDM initiative.
- Held DOL-wide Cybersecurity Awareness Month program as well as other ongoing awareness campaigns, role-based training, and All-Staff notifications to reinforce cybersecurity knowledge.
- Addressed emerging federal information security risks, particularly those targeted by OMB Memoranda released in recent years, such as OMB M-24-10 (*Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*).
- Developed a risk-based approach to identify high-value assets (HVA) through collaborative, data-driven prioritization, which led to resource allocation based on system categorization and ensured the protection of these assets.
- Collaborated with CISA on penetration testing efforts and adopted continuous monitoring to identify previously unknown vulnerabilities. Additionally, DOL continues to participate in the CISA Vulnerability Disclosure Policy (VDP) Platform.
- Achieved an overall "A" on the Federal Information Technology Acquisition Reform Act (FITARA) 18.0 Scorecard, an improvement from a previous "B." The FITARA scorecard, released twice a year, provides a snapshot of the IT strategies of the 24 largest government agencies. DOL exceeded the average score in nearly all categories, including Cybersecurity.

Looking ahead, DOL will continue to focus on strengthening its information security, prioritizing the following:

- Complete adoption of multifactor authentication and encryption of data-at-rest and in-transit.
- Enhance DOL's enterprise log management capability in accordance with OMB M-21-31.
- Implement Security Operations Center enhancements that will allow the Department to anticipate and mitigate risk and stay ahead of the evolving threat landscape.
- Advance the monitoring and protection of critical software and the maturing of capabilities for supply chain risk management.
- Finalize the implementation of data loss prevention tools and alerts.
- Continue efforts to transition DOL's most critical and sensitive networks and systems to quantum resistant cryptography.
- Proceed to increase DOL's capacity to responsibly adopt Artificial Intelligence (AI).
- Continue to transition DOL's network infrastructure to Internet Protocol Version 6.
- Continue the deployment of automation tools and emerging technologies to detect and mitigate cyber threats, to include integrating a zero-trust architecture to better protect resources from unauthorized access.

As demonstrated in the enclosed FISMA report, DOL has implemented a robust information security program and plans to further improve its information security posture consistent with OIG recommendations. The Department recognizes that our work in this space is ongoing due to the ever-evolving nature of the threats.

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](mailto:blahusch.paul.e@dol.gov) or (202) 693-1567. As the CISO, Paul Blahusch is responsible for the corrective actions identified in this correspondence.

cc: Carolyn Angus-Hornbuckle, Assistant Secretary for Administration and Management  
Vince Micone, Deputy Assistant Secretary for Operations  
Paul Blahusch, Chief Information Security Officer  
Muhammad Butt, Division Chief for Cybersecurity Governance