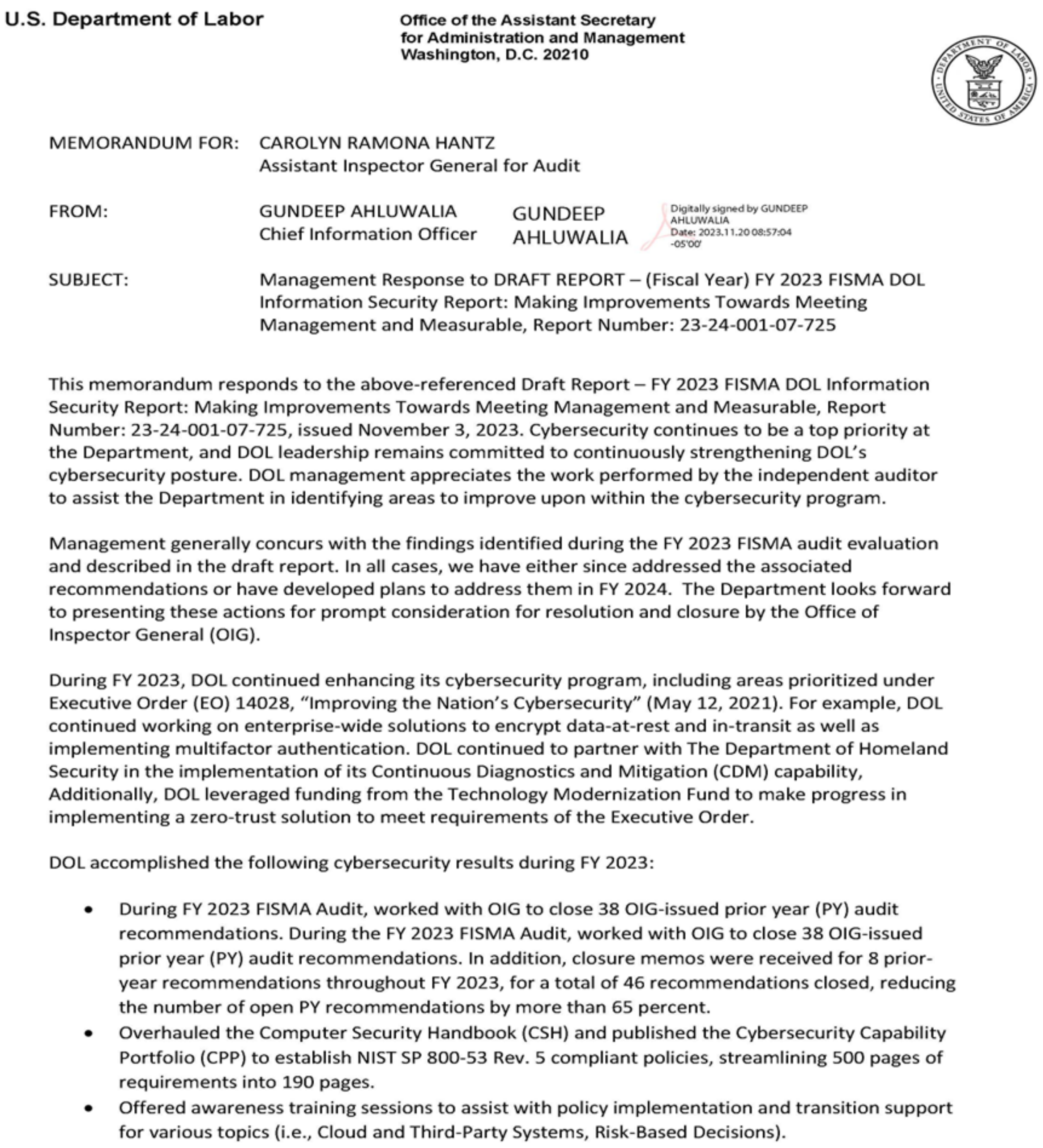
APPENDIX B: AGENCY'S RESPONSE TO THE REPORT



U.S. Department of Labor

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

MEMORANDUM FOR: CAROLYN RAMONA HANTZ
Assistant Inspector General for Audit

FROM: GUNDEEP AHLUWALIA
Chief Information Officer

GUNDEEP AHLUWALIA

Digitally signed by GUNDEEP AHLUWALIA
Date: 2023.11.20 08:57:04 -05'00'

SUBJECT: Management Response to DRAFT REPORT – (Fiscal Year) FY 2023 FISMA DOL Information Security Report: Making Improvements Towards Meeting Management and Measurable, Report Number: 23-24-001-07-725

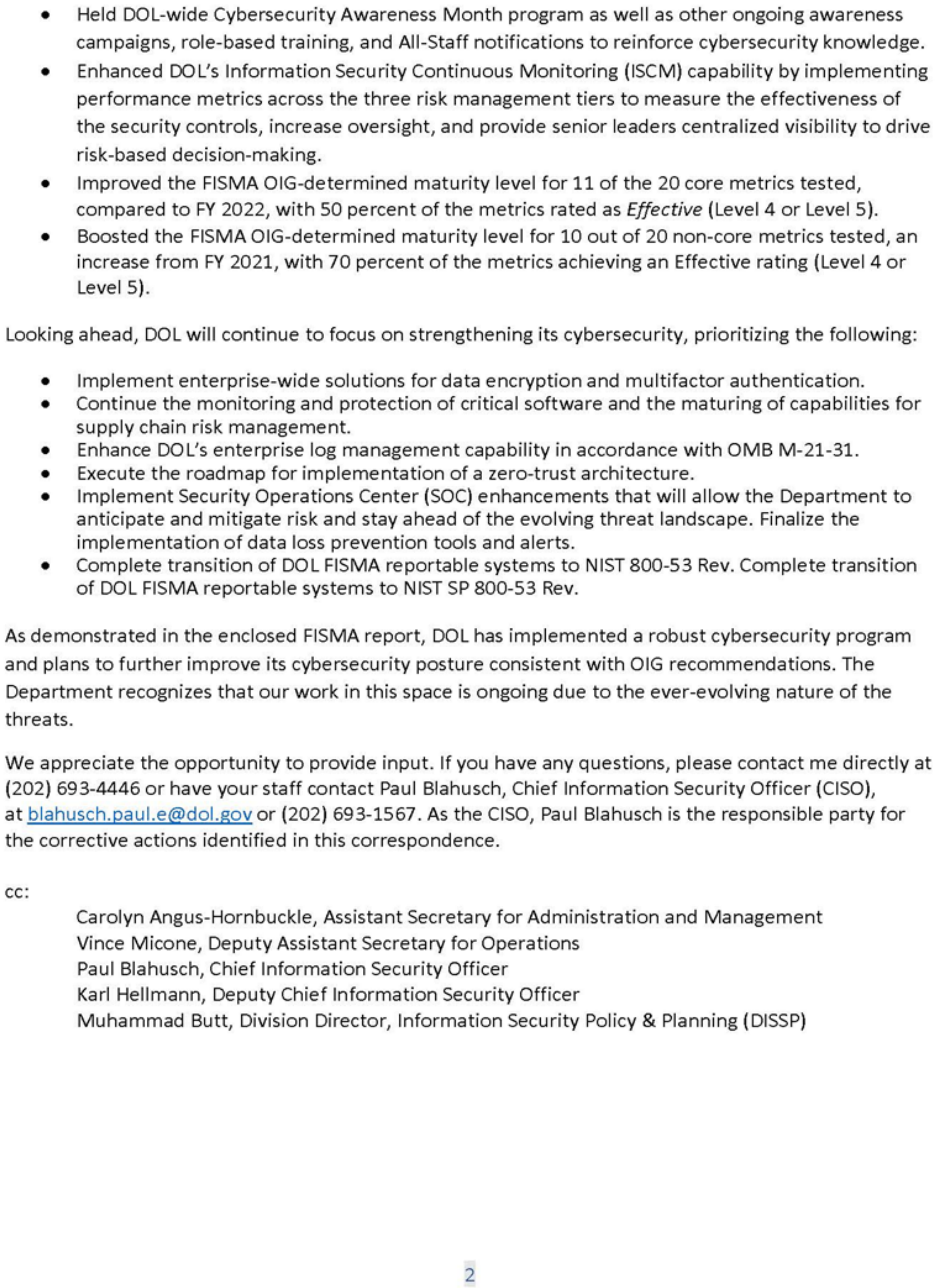
This memorandum responds to the above-referenced Draft Report – FY 2023 FISMA DOL Information Security Report: Making Improvements Towards Meeting Management and Measurable, Report Number: 23-24-001-07-725, issued November 3, 2023. Cybersecurity continues to be a top priority at the Department, and DOL 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 2023 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 2024. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of Inspector General (OIG).

During FY 2023, DOL continued enhancing its cybersecurity program, including areas prioritized under Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" (May 12, 2021). For example, DOL continued working on enterprise-wide solutions to encrypt data-at-rest and in-transit as well as implementing multifactor authentication. DOL continued to partner with The Department of Homeland Security in the implementation of its Continuous Diagnostics and Mitigation (CDM) capability, Additionally, DOL leveraged funding from the Technology Modernization Fund to make progress in implementing a zero-trust solution to meet requirements of the Executive Order.

DOL accomplished the following cybersecurity results during FY 2023:

- During FY 2023 FISMA Audit, worked with OIG to close 38 OIG-issued prior year (PY) audit recommendations. During the FY 2023 FISMA Audit, worked with OIG to close 38 OIG-issued prior year (PY) audit recommendations. In addition, closure memos were received for 8 prior-year recommendations throughout FY 2023, for a total of 46 recommendations closed, reducing the number of open PY recommendations by more than 65 percent.
- Overhauled the Computer Security Handbook (CSH) and published the Cybersecurity Capability Portfolio (CPP) to establish NIST SP 800-53 Rev. 5 compliant policies, streamlining 500 pages of requirements into 190 pages.
- Offered awareness training sessions to assist with policy implementation and transition support for various topics (i.e., Cloud and Third-Party Systems, Risk-Based Decisions).



- 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.
- Enhanced DOL's Information Security Continuous Monitoring (ISCM) capability by implementing performance metrics across the three risk management tiers to measure the effectiveness of the security controls, increase oversight, and provide senior leaders centralized visibility to drive risk-based decision-making.
- Improved the FISMA OIG-determined maturity level for 11 of the 20 core metrics tested, compared to FY 2022, with 50 percent of the metrics rated as *Effective* (Level 4 or Level 5).
- Boosted the FISMA OIG-determined maturity level for 10 out of 20 non-core metrics tested, an increase from FY 2021, with 70 percent of the metrics achieving an Effective rating (Level 4 or Level 5).

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

- Implement enterprise-wide solutions for data encryption and multifactor authentication.
- Continue the monitoring and protection of critical software and the maturing of capabilities for supply chain risk management.
- Enhance DOL's enterprise log management capability in accordance with OMB M-21-31.
- Execute the roadmap for implementation of a zero-trust architecture.
- Implement Security Operations Center (SOC) enhancements that will allow the Department to anticipate and mitigate risk and stay ahead of the evolving threat landscape. Finalize the implementation of data loss prevention tools and alerts.
- Complete transition of DOL FISMA reportable systems to NIST 800-53 Rev. Complete transition of DOL FISMA reportable systems to NIST SP 800-53 Rev.

As demonstrated in the enclosed FISMA report, DOL has implemented a robust cybersecurity program and plans to further improve its cybersecurity 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 or (202) 693-1567. As the CISO, Paul Blahusch is the responsible party 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
Karl Hellmann, Deputy Chief Information Security Officer
Muhammad Butt, Division Director, Information Security Policy & Planning (DISSP)