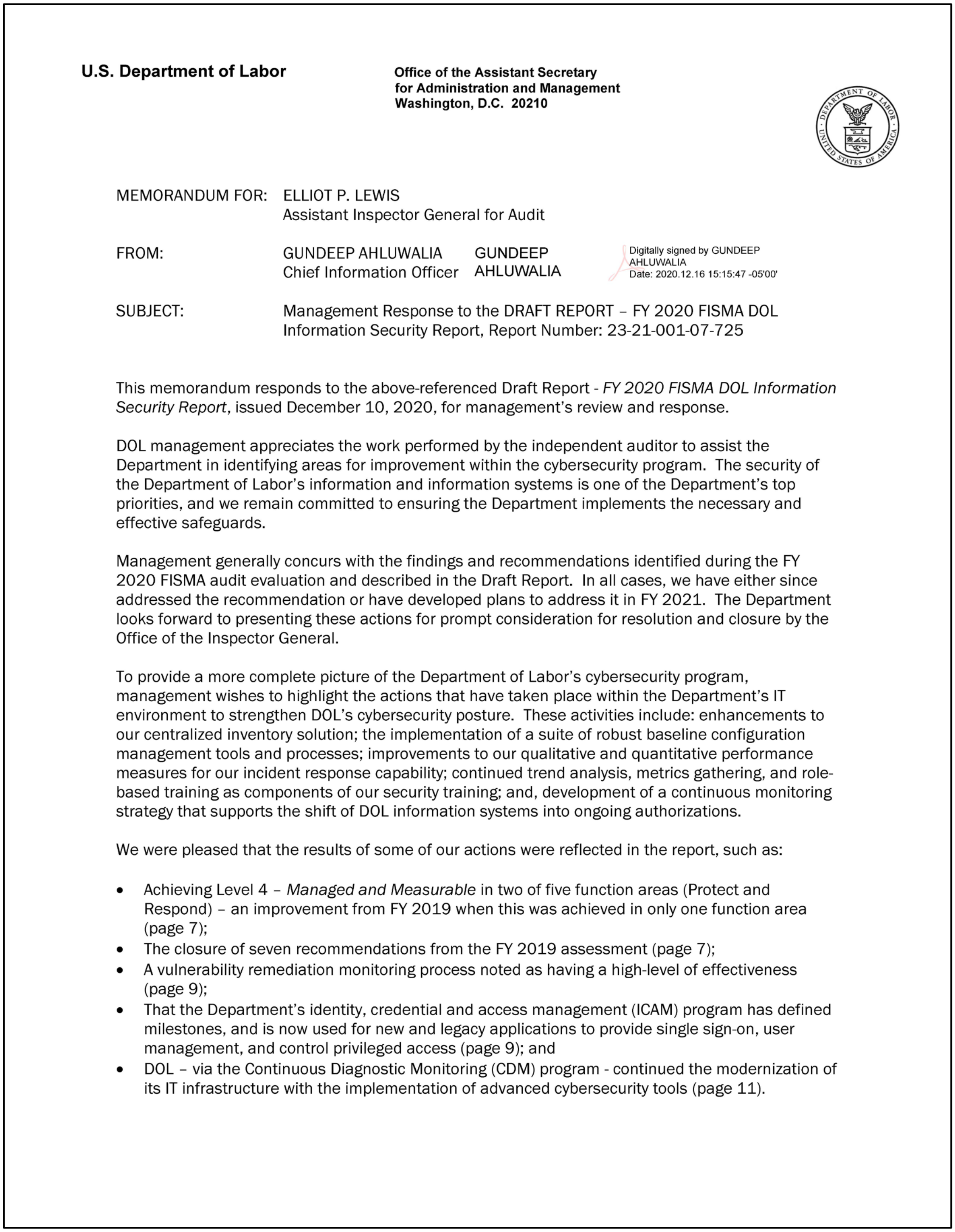
MANAGEMENT'S RESPONSE TO THE REPORT



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

GUNDEEP AHLUWALIA

Digitally signed by GUNDEEP AHLUWALIA
Date: 2020.12.16 15:15:47 -05'00'

SUBJECT: Management Response to the DRAFT REPORT – FY 2020 FISMA DOL Information Security Report, Report Number: 23-21-001-07-725

This memorandum responds to the above-referenced Draft Report - *FY 2020 FISMA DOL Information Security Report*, issued December 10, 2020, for management's review and response.

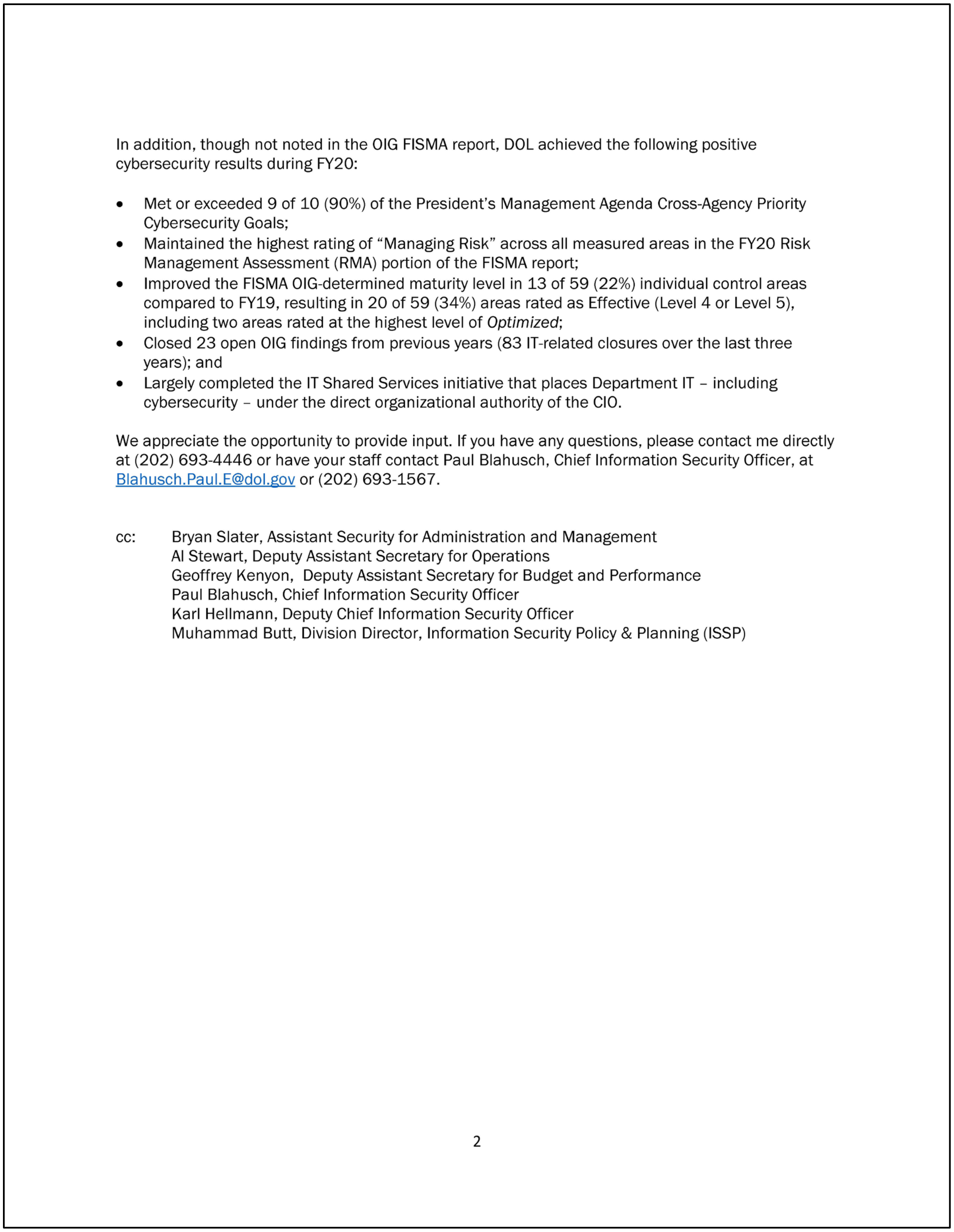
DOL management appreciates the work performed by the independent auditor to assist the Department in identifying areas for improvement within the cybersecurity program. The security of the Department of Labor's information and information systems is one of the Department's top priorities, and we remain committed to ensuring the Department implements the necessary and effective safeguards.

Management generally concurs with the findings and recommendations identified during the FY 2020 FISMA audit evaluation and described in the Draft Report. In all cases, we have either since addressed the recommendation or have developed plans to address it in FY 2021. The Department looks forward to presenting these actions for prompt consideration for resolution and closure by the Office of the Inspector General.

To provide a more complete picture of the Department of Labor's cybersecurity program, management wishes to highlight the actions that have taken place within the Department's IT environment to strengthen DOL's cybersecurity posture. These activities include: enhancements to our centralized inventory solution; the implementation of a suite of robust baseline configuration management tools and processes; improvements to our qualitative and quantitative performance measures for our incident response capability; continued trend analysis, metrics gathering, and role-based training as components of our security training; and, development of a continuous monitoring strategy that supports the shift of DOL information systems into ongoing authorizations.

We were pleased that the results of some of our actions were reflected in the report, such as:

- Achieving Level 4 – *Managed and Measurable* in two of five function areas (Protect and Respond) – an improvement from FY 2019 when this was achieved in only one function area (page 7);
- The closure of seven recommendations from the FY 2019 assessment (page 7);
- A vulnerability remediation monitoring process noted as having a high-level of effectiveness (page 9);
- That the Department's identity, credential and access management (ICAM) program has defined milestones, and is now used for new and legacy applications to provide single sign-on, user management, and control privileged access (page 9); and
- DOL – via the Continuous Diagnostic Monitoring (CDM) program - continued the modernization of its IT infrastructure with the implementation of advanced cybersecurity tools (page 11).



In addition, though not noted in the OIG FISMA report, DOL achieved the following positive cybersecurity results during FY20:

- Met or exceeded 9 of 10 (90%) of the President's Management Agenda Cross-Agency Priority Cybersecurity Goals;
- Maintained the highest rating of "Managing Risk" across all measured areas in the FY20 Risk Management Assessment (RMA) portion of the FISMA report;
- Improved the FISMA OIG-determined maturity level in 13 of 59 (22%) individual control areas compared to FY19, resulting in 20 of 59 (34%) areas rated as Effective (Level 4 or Level 5), including two areas rated at the highest level of *Optimized*;
- Closed 23 open OIG findings from previous years (83 IT-related closures over the last three years); and
- Largely completed the IT Shared Services initiative that places Department IT – including cybersecurity – under the direct organizational authority of the CIO.

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, at Blahusch.Paul.E@dol.gov or (202) 693-1567.

cc: Bryan Slater, Assistant Security for Administration and Management
Al Stewart, Deputy Assistant Secretary for Operations
Geoffrey 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)