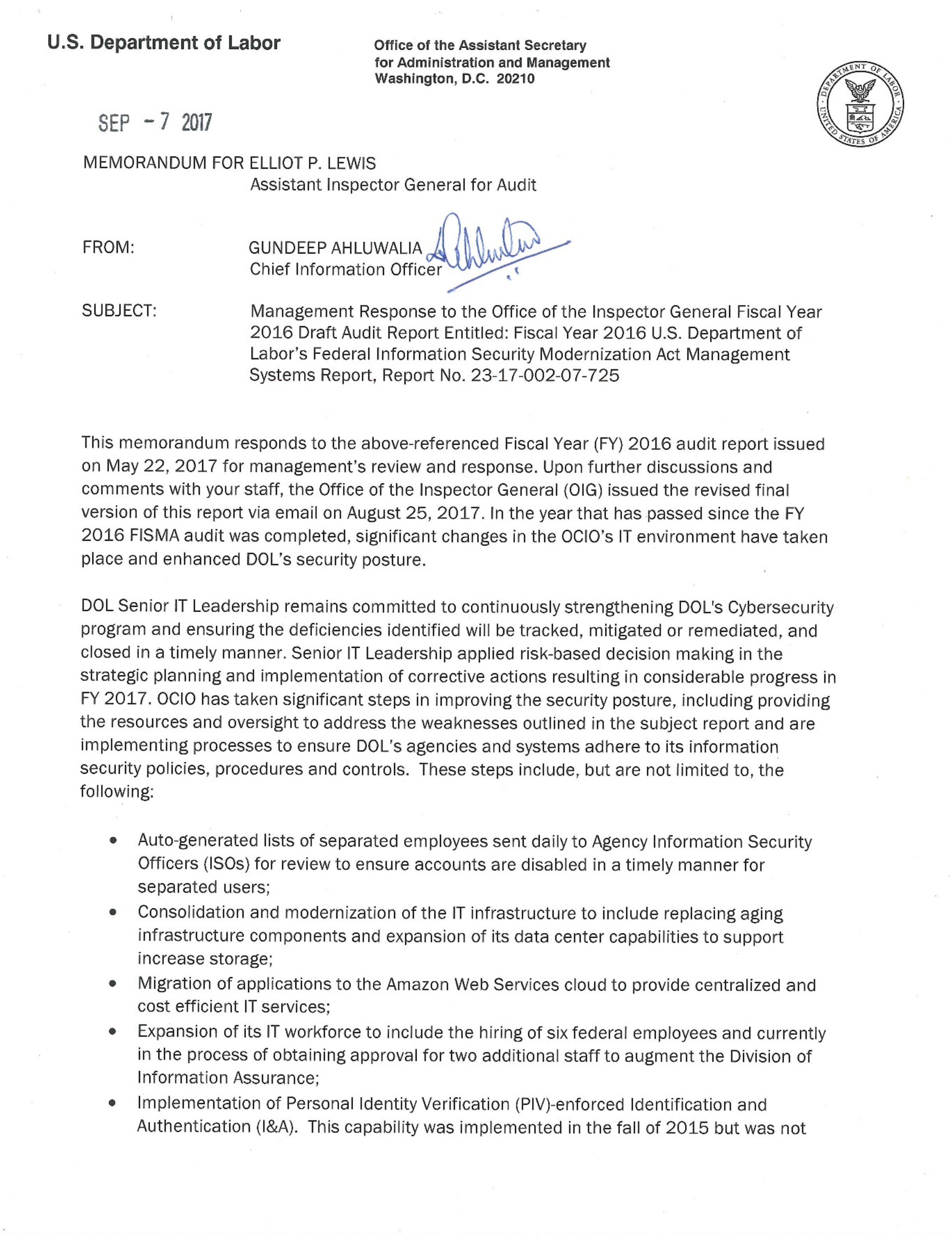


U.S. Department of Labor

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

SEP - 7 2017

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

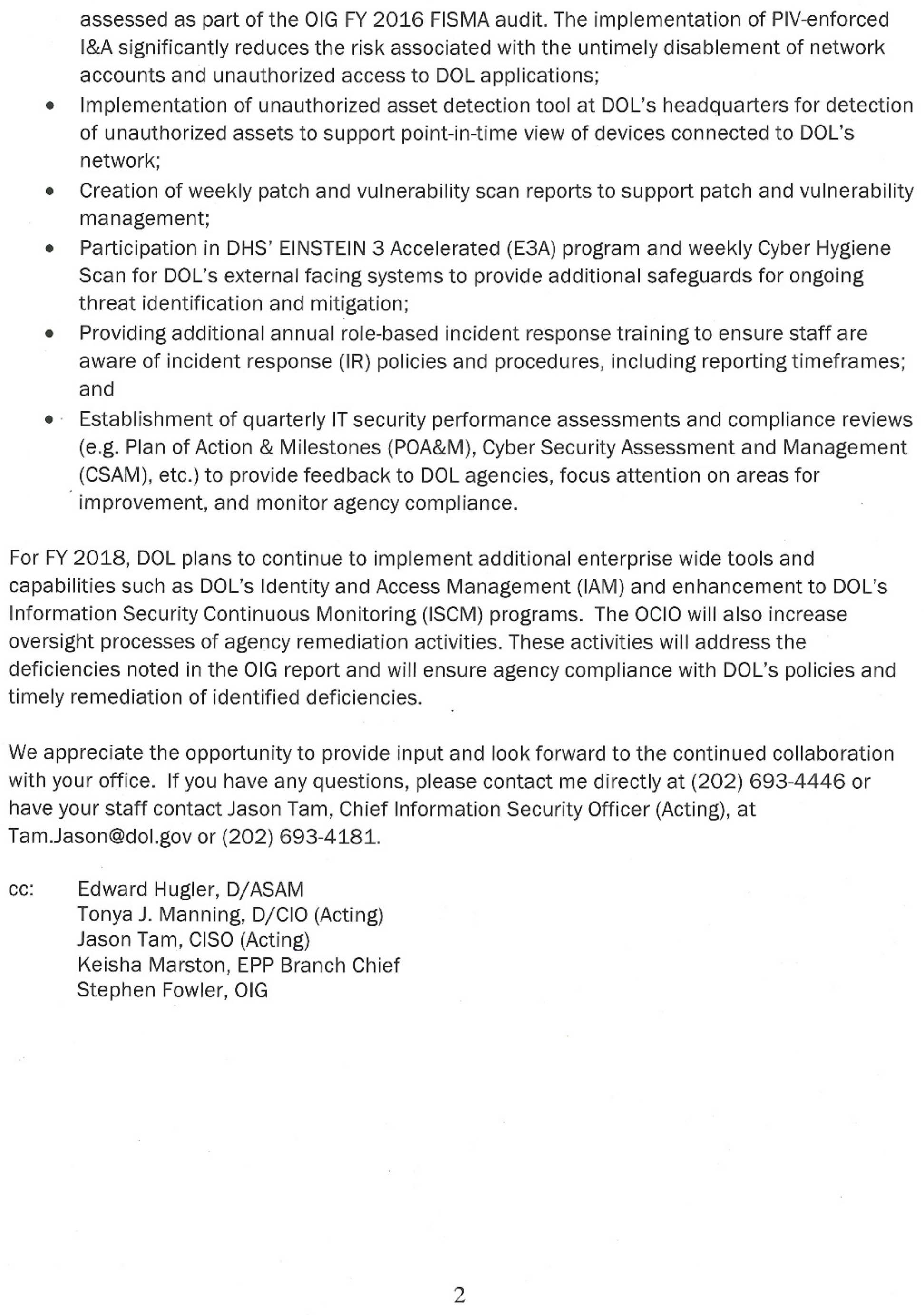
FROM: GUNDEEP AHLUWALIA
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2016 Draft Audit Report Entitled: Fiscal Year 2016 U.S. Department of Labor's Federal Information Security Modernization Act Management Systems Report, Report No. 23-17-002-07-725

This memorandum responds to the above-referenced Fiscal Year (FY) 2016 audit report issued on May 22, 2017 for management's review and response. Upon further discussions and comments with your staff, the Office of the Inspector General (OIG) issued the revised final version of this report via email on August 25, 2017. In the year that has passed since the FY 2016 FISMA audit was completed, significant changes in the OCIO's IT environment have taken place and enhanced DOL's security posture.

DOL Senior IT Leadership remains committed to continuously strengthening DOL's Cybersecurity program and ensuring the deficiencies identified will be tracked, mitigated or remediated, and closed in a timely manner. Senior IT Leadership applied risk-based decision making in the strategic planning and implementation of corrective actions resulting in considerable progress in FY 2017. OCIO has taken significant steps in improving the security posture, including providing the resources and oversight to address the weaknesses outlined in the subject report and are implementing processes to ensure DOL's agencies and systems adhere to its information security policies, procedures and controls. These steps include, but are not limited to, the following:

- Auto-generated lists of separated employees sent daily to Agency Information Security Officers (ISOs) for review to ensure accounts are disabled in a timely manner for separated users;
- Consolidation and modernization of the IT infrastructure to include replacing aging infrastructure components and expansion of its data center capabilities to support increase storage;
- Migration of applications to the Amazon Web Services cloud to provide centralized and cost efficient IT services;
- Expansion of its IT workforce to include the hiring of six federal employees and currently in the process of obtaining approval for two additional staff to augment the Division of Information Assurance;
- Implementation of Personal Identity Verification (PIV)-enforced Identification and Authentication (I&A). This capability was implemented in the fall of 2015 but was not



assessed as part of the OIG FY 2016 FISMA audit. The implementation of PIV-enforced I&A significantly reduces the risk associated with the untimely disablement of network accounts and unauthorized access to DOL applications;

- Implementation of unauthorized asset detection tool at DOL's headquarters for detection of unauthorized assets to support point-in-time view of devices connected to DOL's network;
- Creation of weekly patch and vulnerability scan reports to support patch and vulnerability management;
- Participation in DHS' EINSTEIN 3 Accelerated (E3A) program and weekly Cyber Hygiene Scan for DOL's external facing systems to provide additional safeguards for ongoing threat identification and mitigation;
- Providing additional annual role-based incident response training to ensure staff are aware of incident response (IR) policies and procedures, including reporting timeframes; and
- Establishment of quarterly IT security performance assessments and compliance reviews (e.g. Plan of Action & Milestones (POA&M), Cyber Security Assessment and Management (CSAM), etc.) to provide feedback to DOL agencies, focus attention on areas for improvement, and monitor agency compliance.

For FY 2018, DOL plans to continue to implement additional enterprise wide tools and capabilities such as DOL's Identity and Access Management (IAM) and enhancement to DOL's Information Security Continuous Monitoring (ISCM) programs. The OCIO will also increase oversight processes of agency remediation activities. These activities will address the deficiencies noted in the OIG report and will ensure agency compliance with DOL's policies and timely remediation of identified deficiencies.

We appreciate the opportunity to provide input and look forward to the continued collaboration with your office. 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: Edward Hugler, D/ASAM
Tonya J. Manning, D/CIO (Acting)
Jason Tam, CISO (Acting)
Keisha Marston, EPP Branch Chief
Stephen Fowler, OIG