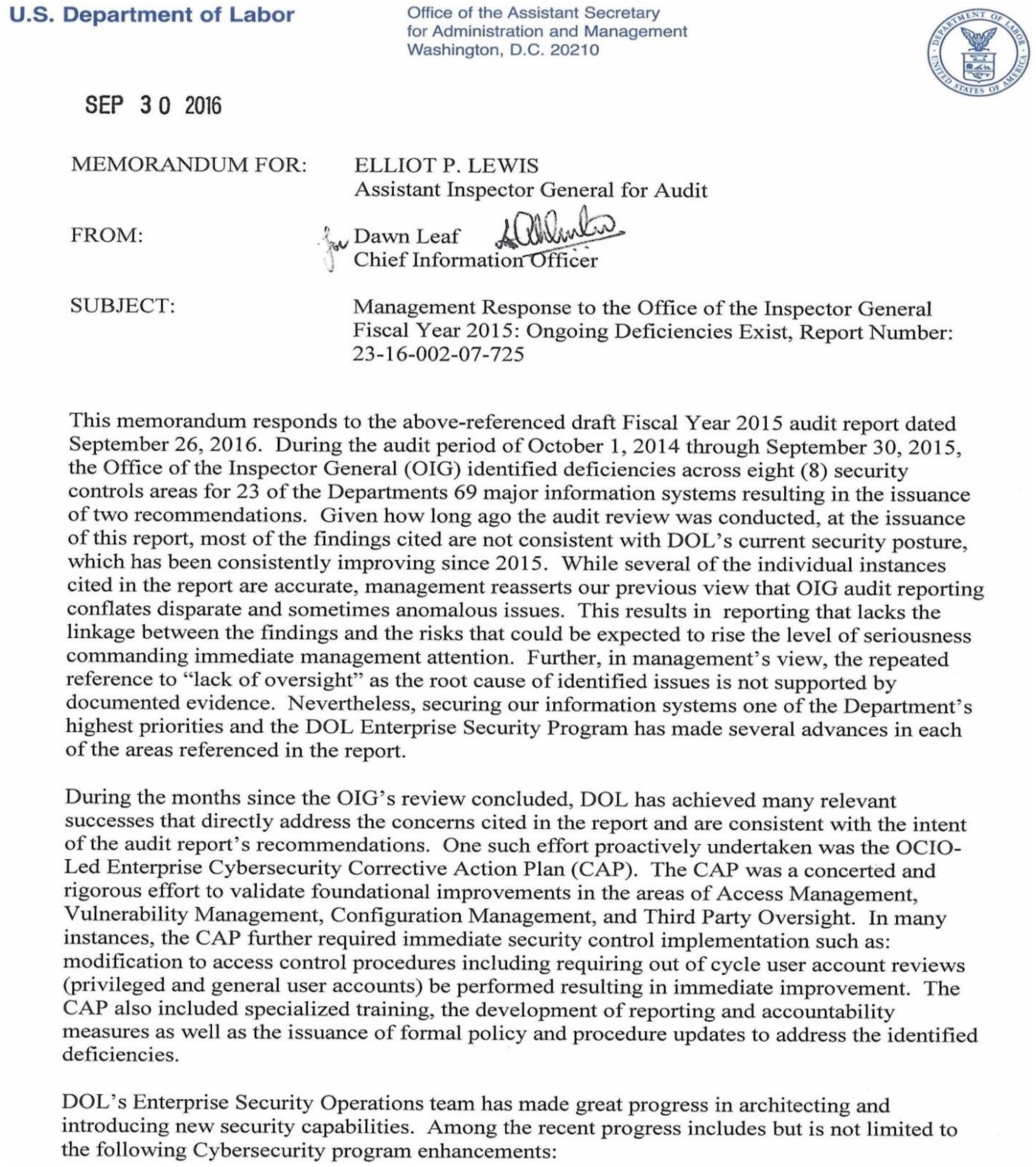
APPENDIX B

MANAGEMENT'S RESPONSE



U.S. Department of Labor

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

SEP 30 2016

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

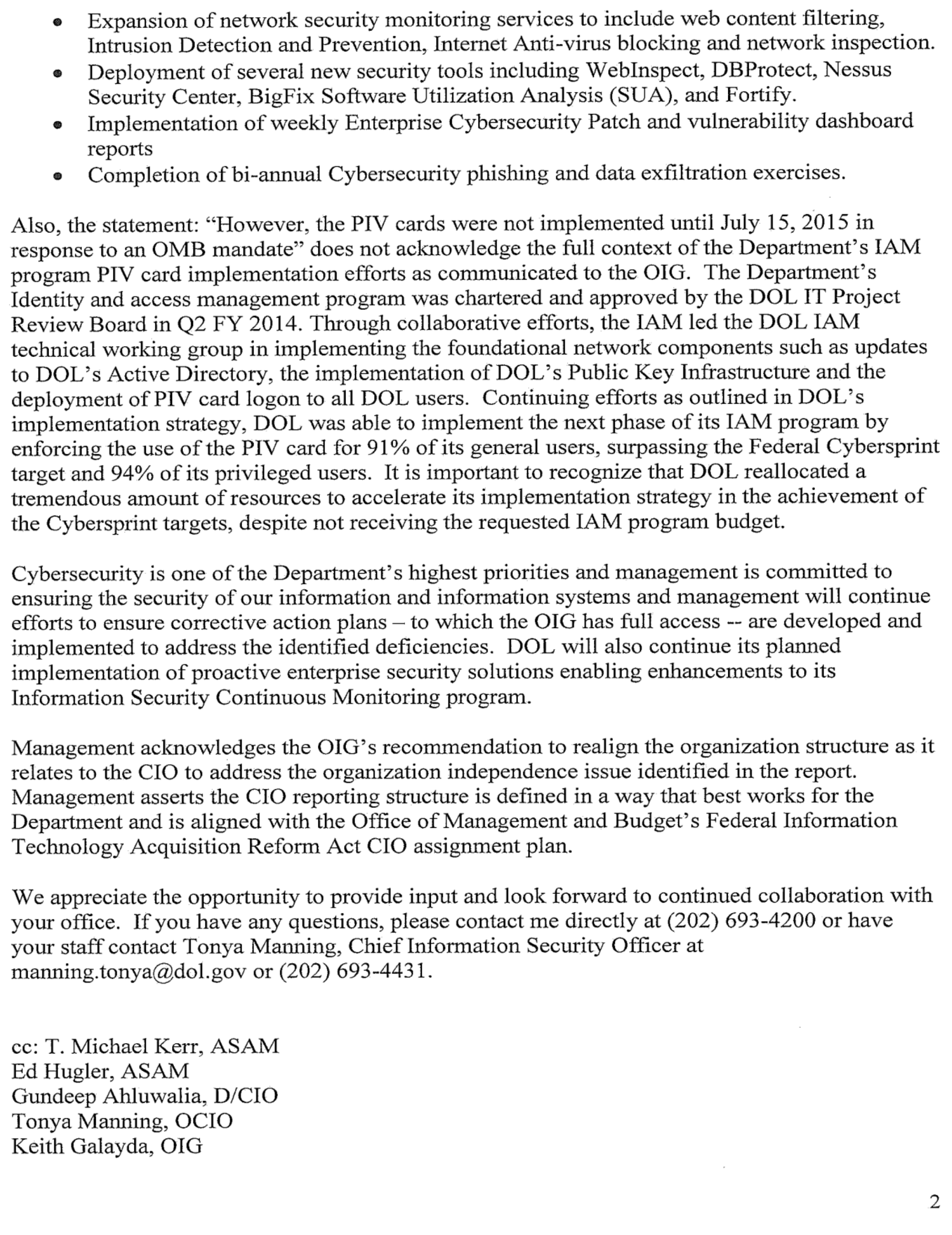
FROM: for Dawn Leaf
Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Fiscal Year 2015: Ongoing Deficiencies Exist, Report Number: 23-16-002-07-725

This memorandum responds to the above-referenced draft Fiscal Year 2015 audit report dated September 26, 2016. During the audit period of October 1, 2014 through September 30, 2015, the Office of the Inspector General (OIG) identified deficiencies across eight (8) security controls areas for 23 of the Departments 69 major information systems resulting in the issuance of two recommendations. Given how long ago the audit review was conducted, at the issuance of this report, most of the findings cited are not consistent with DOL's current security posture, which has been consistently improving since 2015. While several of the individual instances cited in the report are accurate, management reasserts our previous view that OIG audit reporting conflates disparate and sometimes anomalous issues. This results in reporting that lacks the linkage between the findings and the risks that could be expected to rise the level of seriousness commanding immediate management attention. Further, in management's view, the repeated reference to "lack of oversight" as the root cause of identified issues is not supported by documented evidence. Nevertheless, securing our information systems one of the Department's highest priorities and the DOL Enterprise Security Program has made several advances in each of the areas referenced in the report.

During the months since the OIG's review concluded, DOL has achieved many relevant successes that directly address the concerns cited in the report and are consistent with the intent of the audit report's recommendations. One such effort proactively undertaken was the OCIO-Led Enterprise Cybersecurity Corrective Action Plan (CAP). The CAP was a concerted and rigorous effort to validate foundational improvements in the areas of Access Management, Vulnerability Management, Configuration Management, and Third Party Oversight. In many instances, the CAP further required immediate security control implementation such as: modification to access control procedures including requiring out of cycle user account reviews (privileged and general user accounts) be performed resulting in immediate improvement. The CAP also included specialized training, the development of reporting and accountability measures as well as the issuance of formal policy and procedure updates to address the identified deficiencies.

DOL's Enterprise Security Operations team has made great progress in architecting and introducing new security capabilities. Among the recent progress includes but is not limited to the following Cybersecurity program enhancements:



- Expansion of network security monitoring services to include web content filtering, Intrusion Detection and Prevention, Internet Anti-virus blocking and network inspection.
- Deployment of several new security tools including WebInspect, DBProtect, Nessus Security Center, BigFix Software Utilization Analysis (SUA), and Fortify.
- Implementation of weekly Enterprise Cybersecurity Patch and vulnerability dashboard reports
- Completion of bi-annual Cybersecurity phishing and data exfiltration exercises.

Also, the statement: “However, the PIV cards were not implemented until July 15, 2015 in response to an OMB mandate” does not acknowledge the full context of the Department’s IAM program PIV card implementation efforts as communicated to the OIG. The Department’s Identity and access management program was chartered and approved by the DOL IT Project Review Board in Q2 FY 2014. Through collaborative efforts, the IAM led the DOL IAM technical working group in implementing the foundational network components such as updates to DOL’s Active Directory, the implementation of DOL’s Public Key Infrastructure and the deployment of PIV card logon to all DOL users. Continuing efforts as outlined in DOL’s implementation strategy, DOL was able to implement the next phase of its IAM program by enforcing the use of the PIV card for 91% of its general users, surpassing the Federal Cybersprint target and 94% of its privileged users. It is important to recognize that DOL reallocated a tremendous amount of resources to accelerate its implementation strategy in the achievement of the Cybersprint targets, despite not receiving the requested IAM program budget.

Cybersecurity is one of the Department’s highest priorities and management is committed to ensuring the security of our information and information systems and management will continue efforts to ensure corrective action plans – to which the OIG has full access -- are developed and implemented to address the identified deficiencies. DOL will also continue its planned implementation of proactive enterprise security solutions enabling enhancements to its Information Security Continuous Monitoring program.

Management acknowledges the OIG’s recommendation to realign the organization structure as it relates to the CIO to address the organization independence issue identified in the report. Management asserts the CIO reporting structure is defined in a way that best works for the Department and is aligned with the Office of Management and Budget’s Federal Information Technology Acquisition Reform Act CIO assignment plan.

We appreciate the opportunity to provide input and look forward to continued collaboration with your office. If you have any questions, please contact me directly at (202) 693-4200 or have your staff contact Tonya Manning, Chief Information Security Officer at manning.tonya@dol.gov or (202) 693-4431.

cc: T. Michael Kerr, ASAM
Ed Hugler, ASAM
Gundeep Ahluwalia, D/CIO
Tonya Manning, OCIO
Keith Galayda, OIG

2