**<Month Day, Year>**

MEMORANDUM FOR **<Capability>**

SUBJECT: Appointment of Authorizing Official Designated Representative

REFERENCES: (a) Department of Defense Instruction 8510.01, “Risk Management Framework for DoD Information Technology,” dated July 19, 2022

(b) Department of Defense Joint Special Access Program Implementation Guide, dated April 11, 2016; integrated October 8, 2018

(c) Department of Defense Data Strategy, dated September 30, 2020

(d) NIST SP 800-30, Guide for Conducting Risk Assessments, September 2012

(e) NIST SP 800-160v1r1, Engineering Trustworthy Secure Systems, November 2022

(f) Department of Defense Instruction 8140.03, “Cyberspace Workforce Qualification and Management Program,” February 15, 2023

I hereby appoint **<First Name Last Name>** as the primary Authorizing Official Designated Representative (AODR) for all Systems assigned to the **<Capability>** Boundary.

Pursuant to this appointment, the AODR must meet the following requirements:

1. In accordance with reference (a), maintain proper cyberspace workforce qualification ref (f).
2. Advise, on behalf of the Authorizing Official (AO), the Program Manager and Information Owner; they are required to protect all information in accordance with the provisions of the Federal Information Security Modernization Act and any associated security-related federal policies, directives, regulations, standards, and guidance.
3. AODR duties and responsibilities are described in the AO playbooks.
4. As AO, I maintain the authority to revoke this appointment based on lack of due diligence, non-compliance, and/or any other security-related infractions.

Daniel C. Holtzman, SL, CES

Authorizing Official