**<Month Day, Year>**

MEMORANDUM FOR RECORD

FROM: Chief Digital and Artificial Intelligence Office’s (CDAO)Authorizing Official (AO)

SUBJECT: Appointment of Cybersecurity Risk Assessor (CRA)

REFERENCES: (a) DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology, dated July 19, 2022

(b) DoD Joint Special Access Program Implementation Guide, dated April

11, 2016; integrated October 8, 2018

(c) DoD 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) DODI 8140.03, Cyberspace Workforce Qualification and Management Program, 15 February 2023

I hereby appoint **<Name>** as the CRA for **<Provide details>**.

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

1. In accordance with ref (a), maintain proper cyberspace workforce qualification ref (f).
2. Demonstrate the ability to provide risk-based security assessments to support AO authorization determinations.
3. Advise the AO, the Program Manager (PM) and Information Owner on the requirement to protect all information in accordance with the provisions of the Federal Information Security Modernization Act (FISMA) and any applicable associated federal policies, directives, regulations, standards, and guidance.
4. Use the NIST SP 800-30 Guide for Conducting Risk Assessments, ref (d), and Federal, DoD, CDAO directive requirements, as applicable, to assess and monitor cybersecurity risk on a continuous basis.
5. 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 (AO)