**<Month Day, Year>**

MEMORANDUM FOR **<Capability>**

SUBJECT: **<Authorization>,** <**Capability**>, Authorization Termination Date: **<Month Day, Year>**

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

As the appointed Authorizing Official (AO) for the DoD Chief Digital and Artificial Intelligence Office (CDAO), I have determined the **<Capability>** baseline configuration has a residual risk level of **<HIGH, MODERATE, OR LOW>**. Conditions for this **<Authorization>** are provided in Attachment 2. This determination is based on the assessment of the security posture, identified risks, system-specific requirements, proposed and agreed-to mitigations, and all supporting documentation evaluated in accordance with applicable DoD guidance. Key documents from the Body of Evidence reviewed are identified in Attachment 3.

This memorandum serves as the formal authorization for the **<Capability>** baseline and assumes appropriate security measures and/or countermeasures for any identified risks have been properly implemented to provide a satisfactory level of security for operations given the identified risks and tolerances. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the CDAO **<Capability>** CRA as part of the continued risk assessment and authorization process.

Acceptance of this **<Authorization>** by **<Capability>** requires the operating organizations to review, verify, and validate implementation of all policy and processes and site controls as specified, and to identify the inspectable evidence of compliance to the AO via the CDAO **<Capability>** CRA.

I maintain the authority to revoke this Authorization, or any Authorizations to Connect associated, based on lack of due diligence, non-compliance with conditions and policies, and any other security related infractions. The point of contact for this authorization is the CDAO **<CRA>** **<osd.ncr.cdao.mbx.ovl@mail.mil>.**

Daniel C. Holtzman, SL, CES

Authorizing Official

Attachments:

1. Determination Brief

2. Conditions

3. Body of Evidence

4. Capability Categorization Summary

Conditions for the **<Authorization >** for **<Capability>**; Authorization Termination Date (ATD): **<Month Day, Year>**.

1. These conditions are necessary to maintain this Authorization and will be reviewed

**<frequency>**.

|  |  |  |
| --- | --- | --- |
|   | **Condition** | **Due Date** |
| 1. | Conduct AO briefings at an agreed upon cadence outlining current risk status with updates to the AO Determination Brief.  | **<Month Day, Year>** |
| 2. | Monthly regular reviews with the CRA. | Monthly |
| 3. | Execute penetration testing (if needed) of the environment.  | **<Month Day, Year>** |

**Body of Evidence** for the **<Authorization Type>** for **<Capability>;** Authorization Termination Date (ATD): **<Month Day, Year>**.

The Body of Evidence is referenced below. Items **(1)** through **(4)** are key artifacts that supported this recommendation. At Capability’s discretion, the complete package of evidence may be requested through **<Capability POC>**.

List the appropriate references. Example listing, but not limited to:

1. Plan of Actions and Milestones (POA&M)
2. Concept of Operations (CONOPS)
3. Cybersecurity Strategy
4. Incident Response Plan (IRP)
5. Continuous Monitoring Strategy
6. Contingency Plan
7. System Security Plan (SSP)
8. Security Technical Implementation Guide (STIG) Results
9. ACAS Scans
10. Other evidence as required.