**<Month Day, Year>**

MEMORANDUM FOR <**Capability>** AUTHORIZING OFFICIAL (AO)

FROM: Appointed Cyber Risk Assessor (CRA)

SUBJECT: Authorization Recommendation for **<Capability**>

1. As the CRA I have determined that subject Capabilityhas a residual risk level of <**HIGH, MODERATE, LOW**>. Based on the evidence presented, I recommend the <**Authorization Type**> be granted with a termination date of <**Month, Day, Year>.**

1. My recommendation is based on the assessment of the security posture, identified risks, system-specific requirements, and supporting evidence assessed in accordance with the Department of Defense, and best practices. This recommendation assesses the effectiveness of security risk remediation efforts in identifying and mitigating risks, ensuring they achieve the desired level of protection, and confirming that the capability operates as intended.
2. The following conditions are identified in Attachment 1 of the Authorization Memo to further reduce the risk to the Capability and associated data.

**<Name, Position>**

Cyber Risk Assessor

Attachments:

1. Body of Evidence
2. CRA Assessment Report

**Attachment 1**

**Body of Evidence**

The Body of Evidence referenced below are key artifacts that supported this recommendation.

**<List body of evidence used to assess risk within the subject capability>**

**Attachment 2**

**CRA Assessment Report for <Capability>**

1. Security Assessment Results (*Defines findings, vulnerabilities, and weaknesses discovered*)
2. Security Assessment Result Recommendations (*Define finding recommendations*)
3. Security Assessment Methodologies Used (*i.e., Examine, Interview, Test, Cloud, etc.*)
4. Technical Analysis Conducted (*i.e. Cloud, Firewall, CDS, Supply Chain, Zero Trust, Threat modeling, Incident response testing, Penetration testing, vulnerability assessment, etc.*)