Memorandum of Agreement

Between

Department of Defense

<**Capability**>

<**Cyber Risk Assessor**>

and

# Department of Defense

<**Capability**>

# for

# <Capability> and/or Software

# Assessment and Authorization Support

Prepared by: **<Capability>**

**<Month Day Year>**

**1. Purpose**

This Memorandum of Agreement (MOA) specifies an agreement between the **<Capability>** Cyber Risk Assessor (CRA) and the **<Capability>**. This document also defines the responsibilities of the CRA and the Capability, as well as outlining the expected cost associated with an Assessment and Authorization (A&A) activity for capability and or software.

### **2. Background**

The **<Capability>** has received an official determination that their capability and or software is supporting the <Capability> mission area within the Department of Defense (DoD). As directed in Department of Defense Instruction (DoDI) 8510.01, “Risk Management Framework for DoD Systems,” dated July 19, 2022, an Authorizing Official (AO) is required to accept the risk of operating the capability based on a risk assessment provided by an CRA. The **<Capability>** CRA has been appointed to conduct an independent risk assessment for the **<Capability>** AO to make an authorization determination.

**3. Roles and Responsibilities**

**3.1.** TheCRA will:

1. Capability/Software Determination/Categorization Support
   1. Support capability in identifying the proper determination (e.g., capability, product, major application, etc.).
   2. Support the capability in the initial security control selection and categorization guidance contained in National Institute of Standards and Technology (NIST) special publication 800-53 and the Committee on National Security Systems Instruction (CNSSI) 1253 for security controls selection.
   3. Provide guidance to the capability leadership on how to tailor/supplement the initial security control set as needed based on a mission thread and criticality analysis.
2. Security Controls Implementation Planning Support
   1. Provide guidance to the capability Program Manager and ISSM to facilitate the completion, accuracy, and established maintenance schedule of documentation that captures the following: roles/responsibilities of parties that are responsible for implementing the security controls, planned implementation for how controls will be addressed, evaluation of Security Requirements Traceability Matrix (SRTM) or another document that captures the planned implementation.
   2. Evaluate the capability and/or software architecture to ensure accreditation boundaries, data flows, and other system and or software characteristics are defined to support a risk assessment.
   3. Provide technical recommendations to the CRA on the capability security control implementation plan.
3. Assessment Planning and Execution Support
   1. Provide guidance to the capability in developing detailed verification procedures for the previously selected security controls.
   2. Plan and/or participate in the capability’s cyber security-related verification and test meetings to include Readiness Reviews and System Security Working Groups (SSWG), and additional teleconferences as required.
   3. Participate in security control verification activities to include contractor/government testing, vulnerability assessments, and other demonstrations/exercises to validate compliance and conformance with DoD, NIST, user-generated requirements and the capability security control implementation plans.
   4. Provide technical recommendations to the Program Manager and ISSM on verification and assessment methods.
   5. Provide support to the capability on remediation actions resulting from the assessment and or verification activities.
4. Risk Analysis/Mitigation Planning Support
   1. Provide support to the capability to develop a Plan of Action and Milestones (POA&M) based on items that could not be remediated as part of the assessment and or verification activities.
   2. Provide guidance to the capability on the documentation required for an authorization determination or risk assessment.
5. Minor Modification Assessment Support (if planned)
   1. Provide support for tasks stated in section 3.1 for minor modifications to systems/software with existing authorizations.
6. Assessment and Authorization Support
   1. Provide technical recommendations and risk assessments to the CRA and other accrediting authorities as required.
   2. Provide administrative support for assessment recommendations, as well as authorization determination briefing to the CRA and AO (e.g., ATO, IATT, etc.) as required.
   3. Provide assessment and authorization metrics and status of the capability into AO status briefings.
   4. Provide administrative support in data management for assessment artifacts developed.
   5. Provide authorization and assessment support for No Security Impact (NSI) determinations.
7. Continuous Assessment Support
   1. Provide support for quarterly POA&M reviews and annual reassessments of RMF controls.

**3.2** The Capability will:

**3.2.1.** Submit the Military Interdepartmental Purchase Request (MIPR) covering the funding within this MOA. The Capability will also provide the MIPR Number for tracking purposes.

**3.2.2.** Provide an initial capability introductory brief to the AO and CRA.

**3.2.3.** Provide an initial risk assessment report, if one exists, to the CRA.

**3.2.4.** Provide system requirements and information required per DoDI 8510.01, NIST 800-53, any **<Capability>** Standard Processes (for acquisition capabilities) and applicable DoD instruction guidance. A capability milestone schedule will be developed with the capability point of contact (POC) and the CRA.

**3.2.6.** Provide a single POC for the effort.

**3.2.7.** Work in good faith to develop documentation required for the A&A activity.

**3.2.8.** Coordinate independent test/verification of implemented requirements/controls.

**3.2.9.** Provide additional funding as required.

**3.2.10.** Provide all pertinent OVL artifacts, to include previous assessment, scans, code analysis, documentation, and resources.

**3.2.11.** Provide prompt notification of capability changes or issues.

**3.2.12.** Provide scheduled updates to the CRA at least monthly.

**4. Implementation.** The provisions contained within the MOA are effective when signed by the respective approving authorities.

**5. Administrative Information**

**5.1. Points of Contact**

**5.1.1. Capability Contacts (Last name, first name** **<Capability> Program Manager, (781) 225-xxxx, email@mail.mil)**

**5.1.2 <Capability> CRA Contacts** <**Last name, first name** >, Cyber Security Engineering Lead, **<(123) 456-7890, email@mail.mil>**

**5.2 Method of Changing Baseline.** Significant changes in requirements, implementation plans, and verification methods may necessitate changes to documentation (ex. amended Task Utilization Agreement (TUA) or MOA). Requests to update must be sent to the POC’s listed in 5.1.

**5.3. Approval Process for Documentation.** Artifacts requiring CRA, or AO signature take approximately 15 business days to allow for assessor review, peer review, CRA briefing and signature, and AO briefing and signature (if applicable).

**5.4. Capability Period of Performance Covered by this MOA.** Dates from MIPR execution date through <**Day Month Year**>, until termination by mutual consent of signatories, or insufficient capability to meet the funding obligations detailed in this agreement.

**5.4.1 Certification Priority**

**<Capability>:** <**Day Month Year**>, **<Capability> <Authorization Determination**> Continuous Monitoring

**5.5. Financial**

**5.5.1.** Cost Summary

Total Effort: **<Capability>** – **$XXK**

Cost Breakdown:

Activity Cost

Travel TDY (test events/capability meetings) $XX

Security Controls Implementation Planning Support $XX

Risk Analysis/Mitigation Planning Support $XX

Minor Modification Assessment (if applicable) $XX

Assessment and Authorization Support $XX

Continuous Monitoring $XX

**Total $XXK**

Our estimate for direct cost is <**$XX**> (a detailed cost estimate is included in above). Items with zero cost assigned to them are activities out of the scope of this cost estimate. The Capability has not provided funds to cover initial planning and coordination for this tasking. Details on where and how to address the funding will be provided in a separate correspondence.

**6. Agreement and Administration:**

**6.1. Termination date.** This MOA will remain in effect through <**Day Month Year**> or until terminated by mutual consent of the signatories. Additionally, insufficient capability to meet the funding obligations detailed in this agreement will nullify this MOA. Unused funds with be refunded to the capability once de-obligated by the capability.

**6.2. Contracts.** This MOA does not specify the contract, nor contractors used for the assessment tasks outlined in <**Document and Section**>. The **<Procurement Office>** will provide guidance to the **<Capability>** on details regarding the contract and how to transfer funding for the activities contained within this MOA.

**7. Approvals.** We, the undersigned, agree to the responsibilities, cost, period of performance, and support requirements as outlined in this MOA. Change in scope will require our signatures to effect the change. Such changes become a part of this document and are valid from the date said change was signed and funds received.

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| <**First Name Last** > DoD CDAO Cyber Risk Assessor  <**Division**> |  | <**First Name Last**> DoD **<Capability>** Program Manager  <**Division**> |  |