|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Security Assessment and Authorization Plan**  **Document Version: 1.0.0**  **{DATE}** |
| Prepared by: {ORGANIZATION}  **DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.**  **OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" [PDF icon](http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf)
2. DoD Instruction 8500.01, "Cybersecurity", as amended [PDF icon](http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf)
3. Committee on National Security Systems (CNSS) Instruction No. 1253, " Security Categorization and Control Selection for National Security Systems" [PDF icon](https://www.cnss.gov/CNSS/openDoc.cfm?fB+AFcOU6MhwNopIHS6VaQ==)
4. NIST Special Publication 800-53A Revision 4, " Assessing Security and Privacy Controls in Federal Information Systems and Organizations" [PDF icon](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf)
5. NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems" [PDF icon](http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc462575294)

[**2.0** **SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES** 1](#_Toc462575295)

[**3.0** **SECURITY ASSESSMENTS** 2](#_Toc462575296)

[**4.0** **SYSTEM INTERCONNECTIONS** 3](#_Toc462575297)

[**5.0** **SECURITY CERTIFICATION** 3](#_Toc462575298)

[**6.0** **PLAN OF ACTION AND MILESTONES** 3](#_Toc462575299)

[**7.0** **SECURITY AUTHORIZATION** 4](#_Toc462575300)

[**8.0** **CONTINUOUS MONITORING** 4](#_Toc462575301)

[**9.0** **PENETRATION TESTING** 4](#_Toc462575302)

[**10.0** **INTERNAL SYSTEM CONNECTIONS** 4](#_Toc462575303)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 6](#_Toc462575304)

[**ENCLOSURE 1 – INTERCONNECTION SECURITY AGREEMENT TEMPLATE** 51](#_Toc462575305)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc447181008)

# **OVERVIEW**

The objective of security assessment and authorization is to provide guidelines for building effective security assessment plans and a comprehensive set of procedures for assessing the effectiveness of security controls.

The DoD has established an integrated enterprise-wide decision structure for cybersecurity risk management (the Risk Management Framework (RMF)) that includes cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37.

This plan ensures that {ACRONYM} follows the established guidelines and requirements for security assessment and authorization. The formal System Security Plan is documented separately. The purpose of this document is to consolidate information and provide traceability to security control requirements.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix A, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| --- | --- | --- | --- | --- | --- |
| [CA-1](#CA1) | Security Assessment and Authorization Policy and Procedures | P1 | CA-1 | CA-1 | CA-1 |
| [CA-2](#CA2) | Security Assessments | P2 | CA-2 | CA-2 (1) | CA-2 (1) (2) |
| [CA-3](#CA3) | System Interconnections | P1 | CA-3 | CA-3 (5) | CA-3 (5) |
| CA-4 | Security Certification | Not Selected | Not Selected | Not Selected | Not Selected |
| [CA-5](#CA5) | Plan of Action and Milestones | P3 | CA-5 | CA-5 | CA-5 |
| [CA-6](#CA6) | Security Authorization | P2 | CA-6 | CA-6 | CA-6 |
| [CA-7](#CA7) | Continuous Monitoring | P2 | CA-7 | CA-7 (1) | CA-7 (1) |
| [CA-8](#CA8) | Penetration Testing | P2 | Not Selected | Not Selected | CA-8 |
| [CA-9](#CA9) | Internal System Connections | P2 | CA-9 | CA-9 | CA-9 |

Table 1 - SP-800-53v4 Compliance Matrix

# **SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES**

It is {ACRONYM} policy that {ACRONYM} will follow the guidance provided in NIST Special Publication 800-53A Revision 4, " Assessing Security and Privacy Controls in Federal Information Systems and Organizations" for the establishment of security assessment and authorization procedures.

The applicable security assessment and authorization procedures are derived from the System Categorization performed in RMF Step 1, which identifies the applicable requirements and tailoring.

The {ACRONYM} Security Assessment Plan (SAP) contains the scope, roles, responsibilities and coordination activities that are required for successful security assessment. The SAP is required to be updated yearly, or when significant changes occur to {ACRONYM}.

All personnel are required to register with the DTIC website to receive update notifications.

Have all {ACRONYM} registered with the DTIC website?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **SECURITY ASSESSMENTS**

{ACRONYM} security assessments will be performed to ensure that information security is built into the system; identify weaknesses and deficiencies; provide essential information needed to make risk-based decisions as part of security authorization processes; and ensure compliance to vulnerability mitigation procedures. {ACRONYM} assess security controls as part of:

* initial and ongoing security authorizations;
* FISMA annual assessments;
* continuous monitoring; and
* system life cycle activities

{ACRONYM} security assessment will be conducted on the implemented security controls as documented in System Security Plan.

During RMF Step 4 “Assess Security Controls”, an independent Validator is required to perform testing. While the program office may fund the Validator, the Validator will not report directly to the program manager.

Does the Validator report directly to the {ACRONYM} program manager?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

The {ACRONYM} SAP will identify the security controls and those control enhancements under assessment.

Within the {ACRONYM} SAP, is the following information defined:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Are the required security controls and enhancements identified? |  | No |  | Yes |
| 2. | Are the security assessment blocks completed? |  | No |  | Yes |
| 3. | Is the Authorization boundary defined? |  | No |  | Yes |
| 4. | Are the assessment team members and their associated assessment roles and responsibilities listed? |  | No |  | Yes |

The {ACRONYM} Security Assessment Report (SAR) will identify the evaluation status of all security controls.

Within the {ACRONYM} SAR, is the following information defined:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | Are compliance/non-compliance statuses of all controls and specific deficiencies for all non-compliant controls identified? |  | No |  | Yes |
| 3. | Have the ISSO and ISSM received the SAR? |  | No |  | Yes |

# **4.0 SYSTEM INTERCONNECTIONS**

This section applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing.

{ACRONYM} will carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within {ACRONYM} and external to {ACRONYM}. If {ACRONYM} has an interconnection to another system with the same authorizing official, {ACRONYM} do not need to develop an Interconnection Security Agreement. Instead, {ACRONYM} will describe the interface characteristics between those interconnecting systems in the System Security Plan (SSP). If {ACRONYM} has an interconnection to another system with a different authorizing officials, an Interconnection Security Agreements is required.

In the event an Interconnection Security Agreement is required, {ACRONYM} will follow the template found in [Enclosure 1 - Interconnection Security Agreement Template](#_ENCLOSURE_1_–_1), which includes the following information:

* Interface characteristics
* Security requirements
* Nature of information communicated

Does the {ACRONYM} require Interconnection Security Agreements?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, are they reviewed annually?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **5.0 SECURITY CERTIFICATION**

NIST and DoD have not allocated requirements for this subject area.

# **PLAN OF ACTION AND MILESTONES**

The Plan of Action and Milestones (POA&M) is a key document in the {ACRONYM} information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view POA&Ms from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. POA&M updates are based on findings from security control assessments and continuous monitoring activities.

The following process is used by {ACRONYM} to ensure compliance with POA&M requirements:

1. The POA&M is required and will be maintained in eMASS
2. The POA&M will be updated based on assessment and continuous monitoring activities. At a minimum, the eMASS PO&AM will be updated every 90 days
3. All ongoing findings in the POA&M will contain an adequate risk mitigation
4. PO&AM reporting will be executed in accordance with higher-level guidance
5. All {ACRONYM} stakeholders will review the POA&M annually to ensure consistency

# **SECURITY AUTHORIZATION**

Security authorizations are official management decisions, conveyed through authorization decision documents, by senior organizational officials or executives (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls.

Has an Authorizing Official been appointed for {ACRONYM}?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

Has {ACRONYM} been authorized prior to being placed in service?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes, has the security authorization has been updated within the last three years, when there was a significant change to the system, or if there was a change to the environment in which the system operates?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

# **CONTINUOUS MONITORING**

Continuous monitoring facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions.

The {ACRONYM} Continuous Monitoring Strategy implements the process for the required security testing, training, and monitoring activities

Future DoD-wide CM guidance to be published.

# **9.0 PENETRATION TESTING**

{ACRONYM} is not considered a High Impact level, therefore penetration testing is not required.

# **10.0 INTERNAL SYSTEM CONNECTIONS**

This section applies to connections between {ACRONYM} and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, {ACRONYM} will authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Does {ACRONYM} have any internal system connections?

|  |  |
| --- | --- |
|  | No |
|  | Yes |

If Yes,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Connected System | Class or Component | Characteristics | Security Requirements | Nature of Information |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| **Control Number** | **Assessment Number** | **CCI** | **Confidentiality** | **Integrity** | **Availability** | **Assessment Procedures** | **References** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CA-1 | CA-1 (a) | CCI-002061 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (a) | CCI-002062 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the personnel or roles as all personnel. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (a) (1) | CCI-000239 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (a) (1) | CCI-000240 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (a) (2) | CCI-000242 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the procedures to ensure the organization being inspected/assessed develops and documents procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls IAW DoDI 8510.01 | [Section 2](#_SECURITY_ASSESSMENT_AND) |
| CA-1 | CA-1 (a) (2) | CCI-000243 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the AUP (Acceptable Use Policy), appointment orders, or written policy requiring that all personnel register at the DTIC website to receive update notifications.   DoD has defined the personnel or roles as all personnel. | [Section 2](#_SECURITY_ASSESSMENT_AND) |
| CA-1 | CA-1 (b) (1) | CCI-000238 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.    DoD has defined the frequency as every 5 years. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (b) (1) | CCI-000241 | High Moderate Low | High Moderate Low | High Moderate Low | DoDI 8510.01 meets the DoD requirement for security assessment authorization policy and procedures.   DoD Components are automatically compliant with this control because they are covered by the DoD level policy, DoDI 8510.01. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-1 | CA-1 (b) (2) | CCI-000244 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of review and update activity to ensure the organization being inspected/assessed reviews and updates, IAW DoDI 8510.01, the current security assessment and authorization procedures annually. | [Section 2](#_SECURITY_ASSESSMENT_AND) |
| CA-1 | CA-1 (b) (2) | CCI-001578 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-2 (1) | CA-2 (1) | CCI-000255 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the level of independence defined in CA-2 (1), CCI 2064 to ensure that they, as the assessor, meet the required level of independence. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 (1) | CA-2 (1) | CCI-002063 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented level of independence to ensure the organization being inspected/assessed defines the level of independence for assessors or assessment teams to conduct security control assessments of organizational information systems.   DoD has determined the level of independence is not appropriate to define at the Enterprise level. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 (2) | CA-2 (2) | CCI-000256 | High | High | High | The organization conducting the inspection/assessment obtains and examines the test and exercise plan documented in the security assessment plan as well as the results of one or more of the latest security assessments to ensure the organization being inspected/assessed is conducting the assessments required in their security assessment plan annually.   DoD has defined the frequency as annually. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-2 (2) | CA-2 (2) | CCI-001582 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented other forms of security assessments to ensure the organization being inspected/assessed defines other forms of security assessments other than in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment and performance/load testing that should be included as part of security control assessments.   DoD has determined the other forms of security assessments are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-2 (2) | CA-2 (2) | CCI-001583 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented list of security control assessment techniques defined in CA-2 (2), CCI 2064 and verifies that the security assessment plan defines whether the assessment is announced or unannounced. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-2 (2) | CA-2 (2) | CCI-002064 | High | High | High | The organization conducting the inspection/assessment obtains and examines the selected list of assessment techniques that are to be conducted to ensure the selections have been documented. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-2 (2) | CA-2 (2) | CCI-002065 | High | High | High | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-2 (3) | CA-2 (3) | CCI-002067 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems to ensure the organization being inspected/assessed defines the information systems for which they will accept the results of an assessment performed by an external organization.    DoD has determined the information systems are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-2 (3) | CA-2 (3) | CCI-002068 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented external organizations to ensure the organization being inspected/assessed defines the external organizations from which assessment results for organization-defined information systems will be accepted.   DoD has determined the external organizations are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-2 (3) | CA-2 (3) | CCI-002069 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examine the documented requirements to ensure the organization being inspected/assessed defines the requirements the assessments for organization-defined information systems from organization-defined external organizations must meet.   DoD has determined the requirements are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-2 (3) | CA-2 (3) | CCI-002066 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a sampling of records of acceptance or rejection of external organization assessment results to ensure the organization being inspected/assessed accepts the results of an assessment of the information system defined in CA-2 (3), CCI 2067 performed by external organization defined in CA-2 (3), CCI 2068 when the assessment meets requirements defined in CA-2 (3), CCI 2069. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-2 | CA-2 (a) | CCI-000245 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the Security Plan to validate \*security assessment blocks\* are complete. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (a) (1) | CCI-000246 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains the security assessment plan to verify the plan identifies the security controls and those control enhancements under assessment. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (a) (2) | CCI-000247 | High Moderate Low | High Moderate Low | High Moderate Low | DoD components are automatically compliant with this control if using the implementation guidance and validation procedures on the Knowledge Service.   If the organization being inspected/assessed is using alternative implementation guidance and validation procedures, the organization conducting the inspection/assessment will obtain and examine those procedures. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-2 | CA-2 (a) (3) | CCI-000248 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the organization's authorization boundary.   Authorization boundary can be described via one or more of the following: network diagrams, data flow diagrams, system design documents, or a list of information system components. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (a) (3) | CCI-002070 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the security assessment plan to ensure the organization being inspected/assessed lists their assessment team members and their associated assessment roles and responsibilities in the security assessment plan. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (b) | CCI-000251 | High Moderate Low | High Moderate Low | High Moderate Low | See CA-2 c  "The organization conducting the inspection/assessment obtains and examines the security assessment report to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls." | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (b) | CCI-000252 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.    DoD has defined the frequency as annually for technical controls, annually for a portion of management and operation controls such that all are reviewed in a 3-year period except for those requiring more frequent review as defined in other site or overarching policy. NOTE: Technical, Management and Operational is IAW NIST SP 800-53 Table 1-1. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-2 | CA-2 (c) | CCI-000253 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the SAR to verify that it includes the compliance/non-compliance status of all controls and specific deficiencies for all non-compliant controls. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (d) | CCI-000254 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment interviews at a minimum, the ISSO and ISSM to ensure the SAR has been received.   DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM. | [Section 3](#_SECURITY_ASSESSMENTS) |
| CA-2 | CA-2 (d) | CCI-002071 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the individuals or roles as at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-3 (1) | CA-3 (1) | CCI-002073 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines the documented boundary protection device to ensure the organization being inspected/assessed defines the boundary protection device to be used to connect organization-defined unclassified, national security systems to an external network.   DoD has determined the boundary protection device is not appropriate to define at the Enterprise level. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 (1) | CA-3 (1) | CCI-000262 | High Moderate Low |  |  | The organization conducting the inspection/assessment obtains and examines policy document prohibiting direct connection of all unclassified NSS to external networks without the use of a boundary protection device defined in CA-3 (1), CCI 262.   DoD has defined the unclassified, national security systems as all unclassified NSS. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 (1) | CA-3 (1) | CCI-002072 | High Moderate Low |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the unclassified, national security systems as all unclassified NSS. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-3 (2) | CA-3 (2) | CCI-002074 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented boundary protection device to ensure the organization being inspected/assessed defines the boundary protection device to be used for the direct connection of classified, national security system to an external network.   DoD has determined the boundary protection device is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (2) | CA-3 (2) | CCI-000263 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams and examines the information system to ensure the organization being inspected/assessed does not connect any national security systems to an external network without the use of protection devices defined in CA-3 (2), CCI 2074. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (3) | CA-3 (3) | CCI-002076 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented unclassified, non-national security system to ensure the organization being inspected/assessed defines the unclassified, non-national security system that is prohibited from directly connecting to an external network without the use of an organization-defined boundary protection device.   DoD has determined the unclassified, non-national security system is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (3) | CA-3 (3) | CCI-002077 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented boundary protection device to ensure the organization being inspected/assessed defines the boundary protection device to be used to directly connect an organization-defined unclassified, non-national security system to an external network.   DoD has determined the boundary protection device is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (3) | CA-3 (3) | CCI-002075 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams and examines the information system to ensure the organization being inspected/assessed does not connect any national security systems to an external network without the use of protection devices defined in CA-3 (3), CCI 2077. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (4) | CA-3 (4) | CCI-002079 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system to ensure the organization being inspected/assessed defines the information system that is prohibited from directly connecting to a public network.   DoD has determined the information system is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (4) | CA-3 (4) | CCI-002078 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines network topology diagrams and examines the information system to ensure the organization being inspected/assessed does not connect any information system defined in CA-3 (4), CCI 2079 to a public network. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-3 (5) | CA-3 (5) | CCI-002082 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed selects deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems.  DoD has defined the information systems as any systems requiring external connectivity. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 (5) | CA-3 (5) | CCI-002081 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the information systems as any systems requiring external connectivity. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-3 (5) | CA-3 (5) | CCI-002080 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment examines the information system to ensure the organization being inspected/assessed configures the information system to employ a deny-all, permit by exception policy for allowing any systems requiring external connectivity to connect to external information systems.   For information system components that have applicable STIGs or SRGs, the organization conducting the inspection/assessment evaluates the components to ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs pertaining to CCI 2080.  DoD has defined the information systems as any systems requiring external connectivity. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (a) | CCI-000257 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines documentation of the Interconnection Security Agreements to include appropriate signatures.     Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (b) | CCI-000258 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation.     Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (b) | CCI-000259 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines interconnection security agreement documentation, specifically looking at any additional security controls identified for  implementation.     Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (b) | CCI-000260 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the interconnection security agreement documentation, specifically to identify the type of information being transferred/transmitted.   Characteristics will include but are not limited to: classification, information type (e.g. PII, HIPAA, FOUO, financial data, etc.)     Policy Note: Interconnection security agreements are required for systems connecting between enclaves that require the hosting enclave to enable PPS outside of their already established and approved business practices. Connections can include both DoD enclaves or non DoD enclaves. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (c) | CCI-002083 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of reviews and updates to ensure the organization being inspected/assessed reviews and updates Interconnection Security Agreements at least annually.   DoD has defined the frequency as at least annually. | [Section 4](#_4.0_SYSTEM_INTERCONNECTIONS) |
| CA-3 | CA-3 (c) | CCI-002084 | High Moderate Low | High Moderate Low |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.   DoD has defined the frequency as at least annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-5 (1) | CA-5 (1) | CCI-000267 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms.   The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-5 (1) | CA-5 (1) | CCI-000268 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms.   The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-5 (1) | CA-5 (1) | CCI-000269 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation of the use of the identified automated mechanisms.   The organization being inspected/assessed may be required to demonstrate use of their identified automated mechanisms. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-5 | CA-5 (a) | CCI-000264 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the security POA&M for compliance with DoDI 8510.01. | [Section 6](#_PLAN_OF_ACTION) |
| CA-5 | CA-5 (b) | CCI-000266 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines current POA&M. The objective is to validate the organization is providing updates to the POA&M at least every 90 days. Review of POA&M without change must be documented (i.e., adding review date to the POA&M header information).   DoD has defined the frequency as at least every 90 days. | [Section 6](#_PLAN_OF_ACTION) |
| CA-5 | CA-5 (b) | CCI-000265 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.    DoD has defined the frequency as at least every 90 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-6 | CA-6 (a) | CCI-000270 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the written appointment memorandum. | [Section 5](#_5.0_SECURITY_CERTIFICATION) |
| CA-6 | CA-6 (b) | CCI-000271 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the authorization document to ensure the information system is authorized prior to being placed into operational status. | [Section 5](#_5.0_SECURITY_CERTIFICATION) |
| CA-6 | CA-6 (c) | CCI-000272 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the security authorization documentation to confirm the security authorization has been updated within the last three years, when there was a significant change to the system, or if there was a change to the environment in which the system operates.   DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. | [Section 5](#_5.0_SECURITY_CERTIFICATION) |
| CA-6 | CA-6 (c) | CCI-000273 | High Moderate Low | High Moderate Low | High Moderate Low | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level.    DoD has defined the frequency as at least every three years, whenever there is a significant change to the system, or if there is a change to the environment in which the system operates. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-7 | CA-7 | CCI-000274 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 (1) | CA-7 (1) | CCI-000282 | High Moderate | High Moderate | High Moderate | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 (1) | CA-7 (1) | CCI-002085 | High Moderate | High Moderate | High Moderate | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 (3) | CA-7 (3) | CCI-002086 | blank | blank | blank | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (a) | CCI-002087 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (b) | CCI-002088 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (b) | CCI-002089 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (c) | CCI-000279 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (d) | CCI-002090 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (e) | CCI-002091 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (f) | CCI-002092 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (g) | CCI-000281 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (g) | CCI-001581 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-7 | CA-7 (g) | CCI-000280 | High Moderate Low | High Moderate Low | High Moderate Low | Future DoD-wide CM guidance to be published | N/A. Awaiting future DoD-wide CM guidance to be published |
| CA-8 | CA-8 | CCI-002094 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency for conducting penetration testing on organization-defined information systems or system components.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-8 | CA-8 | CCI-002095 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components on which penetration testing will be conducted.   DoD has determined the information systems or system components are not appropriate to define at the Enterprise level. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-8 | CA-8 | CCI-002093 |  | High |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of the penetration test results to ensure the organization being inspected/assessed conducts penetration testing in accordance with the frequency defined in CA-8, CCI 2094 on information systems or system components defined in CA-8, CCI 2095. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| CA-8 (1) | CA-8 (1) | CCI-002096 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines a sampling of the penetration test results to ensure the organization being inspected/assessed employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-8 (2) | CA-8 (2) | CCI-002097 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented red team exercises to ensure the organization being inspected/assessed defines red team exercises to simulate attempts by adversaries to compromise organizational information systems.   DoD has determined the red team exercises are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-8 (2) | CA-8 (2) | CCI-002098 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented rules of engagement to ensure the organization being inspected/assessed defines the rules of engagement for red team exercise to simulate attempts by adversaries to compromise organizational information systems.   DoD has determined the rules of engagement are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-8 (2) | CA-8 (2) | CCI-002099 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of red team exercises and results to ensure the organization being inspected/assessed employs red team exercises defined in CA-8 (2), CCI 2097 to simulate attempts by adversaries to compromise organizational information systems in accordance with rules of engagement defined in CA-8 (2), CCI 2098. | Automatically compliant with this CCI because they are covered at the DoD level |
| CA-9 (1) | CA-9 (1) | CCI-002100 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of security compliance checks to ensure the organization being inspected/assessed performs security compliance checks on constituent components prior to the establishment of the internal connection. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| CA-9 | CA-9 (a) | CCI-002101 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the audit trail of authorizations to ensure the organization being inspected/assessed authorizes internal connections of information system components defined in CA-9, CCI 2102 or classes of components to the information system. | [Section 8](#_8.0_INTERNAL_SYSTEM) |
| CA-9 | CA-9 (a) | CCI-002102 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented information system components to ensure the organization being inspected/assessed defines the information system components or classes of components that that are authorized internal connections to the information system.   DoD has determined the information system components are not appropriate to define at the Enterprise level. | [Section 8](#_8.0_INTERNAL_SYSTEM) |
| CA-9 | CA-9 (b) | CCI-002103 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented interface characteristics as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the interface characteristics. | [Section 8](#_8.0_INTERNAL_SYSTEM) |
| CA-9 | CA-9 (b) | CCI-002104 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented security requirements as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the security requirements. | [Section 8](#_8.0_INTERNAL_SYSTEM) |
| CA-9 | CA-9 (b) | CCI-002105 | High Moderate Low | High Moderate Low |  | The organization conducting the inspection/assessment obtains and examines the documented nature of information communication as well as the network topology to ensure the organization being inspected/assessed documents, for each internal connection, the nature of the information communicated. | [Section 8](#_8.0_INTERNAL_SYSTEM) |

# **ENCLOSURE 1 – INTERCONNECTION SECURITY AGREEMENT TEMPLATE**

**1.0 Interconnection Statement of Requirements**

Use this section to document the formal requirement for connecting the two systems. Explain the rationale for the interconnection to the two DAAs. Enter a one- or two-paragraph statement justifying the interconnection. Within the information presented, include the following information:

1. The requirement for the interconnection, including the benefits derived.
2. The names of the systems being interconnected.
3. The agency name or organization that initiated the requirement.
4. If the requirement is generated by a higher level agency or organization, indicate the name of the organization and the individual, if appropriate, that requested the interconnection.

**2.0 System Security Considerations**

Use this section to document the security features that are in place to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. The technical representative from each organization should discuss the contents on this section to come to a mutual agreement as to which items will be included. Both organizations should answer each item, even if only one party is affected by the item in question.

The following items should be addressed:

General Information/Data Description. Describe the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems

Services Offered. Describe the nature of the information services (e.g., e-mail, file transfer protocol [FTP], database query, file query, general computational services) offered over the interconnection by each organization.

Data Sensitivity. Enter the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved (e.g., Privacy Act, Trade Secret Act, Law Enforcement Sensitive, Sensitive-But-Unclassified) and the most restrictive protection measures required.

User Community. Describe the “user community” that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, discuss requirements for background investigations and security clearances, if appropriate.

Information Exchange Security. Describe all system security technical services pertinent to the secure exchange of data between the connected systems.

Rules of Behavior. Summarize the aspects of behavior expected from users who will have access to the interconnection. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering, and viruses, among others. Do not enter statements of law or policy. Such statements typically are addressed in the MOU/A.

Formal Security Policy. Enter the titles of the formal security policy(ies) that govern each system (e.g., “Information Systems Policy and Procedures, Number xxxx” for “Organization A”).

Incident Reporting. Describe the agreements made regarding the reporting of and response to information security incidents for both organizations. For example, “Each organization will report incidents in accordance to its own (procedure name) procedures.” If no incident reporting is performed, so state.

Audit Trail Responsibilities. Describe how the audit trail responsibility will be shared by the organizations and what events each organization will log. Specify the length of time that audit logs will be retained. If no audit trail is performed, so state.

**3.0 Topological Drawing**

Include a topological drawing illustrating the interconnectivity from one system to the other system (end-point to end-point). The drawing should include the following:

* All communications paths, circuits, and other components used for the interconnection, from “Organization A’s” system to “Organization B’s” system.
* The drawing should depict the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations).
* If required, mark the top and bottom of each page with an appropriate handling requirement, such as “FOR OFFICIAL USE ONLY” or “FOR INTERNAL USE ONLY”.

**4.0 Signatory Authority**

Include a signature line. Optionally, this section may include any statements that the two DAAs desire in order to finalize the ISA. This section should include the following:

* The expiration date of the agreement
* Periodic review requirements, such as the date of the next review
* Other statements as required by the DAAs, if any
* The signatures of the DAAs from each organization, and the date of the signatures