|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}**  **eMASS# {EMASS#}**  **Confidentiality: {CONFIDENTIALITY}**  **Integrity: {INTEGRITY}**  **Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Risk Assessment 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. NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments" [PDF icon](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)

**Table of Contents**

[**1.0** **OVERVIEW** 1](#_Toc461416746)

[**2.0** **RISK ASSESSMENT POLICY AND PROCEDURES** 1](#_Toc461416747)

[**3.0** **SECURITY CATEGORIZATION** 1](#_Toc461416748)

[**4.0** **RISK ASSESSMENT** 2](#_Toc461416749)

[**5.0** **VULNERABILITY SCANNING** 3](#_Toc461416750)

[**APPENDIX A – DETAILED COMPLIANCE MATRIX** 6](#_Toc461416751)

[**ENCLOSURE 1 – RISK ASSESSMENT REPORT TEMPLATE** 21](#_Toc461416752)

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

# **OVERVIEW**

The purpose of this Risk Assessment Plan is to provide guidance for conducting risk assessments. This plan ensures that {ACRONYM} follows and implements the [NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments”](http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf).

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_–).

The following Assessment Procedures have not been allocated by NIST:

* RA-4: Risk Assessment Update
* RA-6: Technical Surveillance Countermeasures Survey

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [RA-1](#RA1) | Risk Assessment Policy and Procedures | P1 | RA-1 | RA-1 | RA-1 |
| [RA-2](#RA2) | Security Categorization | P1 | RA-2 | RA-2 | RA-2 |
| [RA-3](#RA3) | Risk Assessment | P1 | RA-3 | RA-3 | RA-3 |
| RA-4 | Risk Assessment Update | Not Selected | Not Selected | Not Selected | Not Selected |
| [RA-5](#RA5) | Vulnerability Scanning | P1 | RA-5 | RA-5 (1) (2) (5) | RA-5 (1) (2) (4) (5) |
| [RA-6](#RA6) | Technical Surveillance Countermeasures Survey | P0 | Not Selected | Not Selected | Not Selected |

Table 1 - SP-800-53v4 Compliance Matrix

# **RISK ASSESSMENT POLICY AND PROCEDURES**

DoD Components are automatically compliant with risk assessment policies and procedures because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.

DoD has defined the personnel or roles for risk assessment policies and procedures roles as at a minimum, the ISSM and ISSO.

DoD has defined the frequency for risk assessment policies and procedures updates as annually - updated as appropriate.

# **SECURITY CATEGORIZATION**

Security categorization describe the potential adverse impacts to {ACRONYM} operations, assets, and individuals if {ACRONYM} is comprised through a loss of confidentiality, integrity, or availability.

Has {ACRONYM} completed RMF Step 1 – System Categorization?

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

If Yes, are categorization results (including supporting rationale) in the security plan?

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

If Yes, has the security categorization decision been reviewed and approved by the authorizing official or authorizing official designated representative?

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

# **RISK ASSESSMENT**

Risk assessments take into account threats, vulnerabilities, likelihood, and impact to {ACRONYM} operations and assets, individuals, other organizations, and the Nation based on the operation and use of {ACRONYM}.

{ACRONYM} will create a Risk Assessment Report (RAR) that contains an executive summary; detailed risk assessment results; and supporting appendices. A RAR Template is provided in [Enclosure 1](#_Enclosure_1_–) and contains the following information:

* Executive Summary
  + List the date of the risk assessment
  + Summarize the purpose of the risk assessment
  + Describe the scope of the risk assessment
  + State whether this is an initial or subsequent risk assessment. If a subsequent risk assessment, state the circumstances that prompted the update and include a reference to the previous Risk Assessment Report
  + Describe the overall level of risk (e.g., Very Low, Low, Moderate, High, or Very High)
  + List the number of risks identified for each level of risk (e.g., Very Low, Low, Moderate, High, or Very High)
* Body of the Report
  + Describe the purpose of the risk assessment, including questions to be answered by the assessment
  + Identify assumptions and constraints
  + Describe risk tolerance inputs to the risk assessment (including the range of consequences to be considered)
  + Identify and describe the risk model and analytic approach; provide a reference or include as an appendix, identifying risk factors, value scales, and algorithms for combining values
  + Provide a rationale for any risk-related decisions during the risk assessment process
  + Describe the uncertainties within the risk assessment process and how those uncertainties influence decisions
  + If the risk assessment includes organizational missions/business functions, describe the missions/functions (e.g., mission/business processes supporting the missions/functions, interconnections and dependencies among related missions/business functions, and information technology that supports the missions/business functions)
  + If the risk assessment includes organizational information systems, describe the systems (e.g., missions/business functions the system is supporting, information flows to/from the systems, and dependencies on other systems, shared services, or common infrastructures)
  + Summarize risk assessment results (e.g., using tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g., number of threat events for different combinations of likelihood and impact, the relative proportion of threat events at different risk levels)
  + Identify the time frame for which the risk assessment is valid (i.e., time frame for which the assessment is intended to support decisions)
  + List the risks due to adversarial threats
  + List the risks due to non-adversarial threats
* Appendices
  + List references and sources of information
  + List the team or individuals conducting the risk assessment including contact information
  + List risk assessment details and any supporting evidence

Has an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of {ACRONYM} and the information it processes, stores, or transmits been performed?

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

Has the Risk Assessment Report been created?

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

Have the risk assessment results been updated upon re-accreditation or whenever there are significant changes to {ACRONYM} or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of {ACRONYM}?

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

Has the Risk Assessment Report been disseminated to the ISSM, ISSO, AO, and PM?

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

# **5.0 VULNERABILITY SCANNING**

Vulnerability scanning includes, for example: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms. {ACRONYM} will utilize, at a minimum, the following DoD provided tools for vulnerability scanning:

* Assured Compliance Assessment Solution (ACAS)
* Security Content Automation Protocol (SCAP)

{ACRONYM} will follow the DISA process for performing ACAS scans, which is located at <https://patches.csd.disa.mil/CollectionInfo.aspx?id=535>.

{ACRONYM} will follow the DISA process for performing SCAP scans, which is located at <http://iase.disa.mil/stigs/scap/Pages/index.aspx>.

Is {ACRONYM} utilizing ACAS and SCAP for vulnerability scanning?

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

If Yes, is ACAS and SCAP configured to use the latest DISA-provided policies and updates?

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

If Yes, is ACAS and SCAP configured to use privileged accounts for scanning?

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

The following figure defines the overarching vulnerability scanning process and provides the following information:

* corrective actions when information about {ACRONYM} is discoverable by adversaries
* ensure that the organization being inspected/assessed has configured the information system in compliance with the applicable STIGs and SRGs
* identify and report new vulnerabilities
* remediation of legitimate vulnerabilities

Vulnerability scanning will occur every **30/90** days and the results shared with at a minimum, the ISSM and ISSO.



# **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** | **Tier** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| RA-1 | RA-1 (a) | CCI-002368 | 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 at a minimum, the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (a) | CCI-002369 | 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 at a minimum, the ISSM and ISSO. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (a) (1) | CCI-001037 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (a) (1) | CCI-001038 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (a) (2) | CCI-001041 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (a) (2) | CCI-001042 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (b) (1) | CCI-001039 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (b) (1) | CCI-001040 | 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 reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (b) (2) | CCI-001043 | High Moderate Low | High Moderate Low | High Moderate Low | NIST SP 800-30 meets the DoD requirements for risk assessment policy and procedures.   DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-1 | RA-1 (b) (2) | CCI-001044 | High Moderate Low | High Moderate Low | High Moderate Low | DoD Components are automatically compliant with this CCI because they are covered by the DoDi 8510.01 which adopts NIST SP 800-30 as the DoD risk assessment policy.  DoD has defined the frequency as annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-2 | RA-2 (a) | CCI-001045 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed categorizes information and the information system in accordance with CNSSI 1253 and applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. | [Section 3](#_SECURITY_CATEGORIZATION) |
| RA-2 | RA-2 (b) | CCI-001046 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented security categorization results to ensure the organization being inspected/assessed documents the security categorization results (including supporting rationale) in the security plan for the information system IAW CNSSI 1253. | [Section 3](#_SECURITY_CATEGORIZATION) |
| RA-2 | RA-2 (c) | CCI-001047 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. | [Section 3](#_SECURITY_CATEGORIZATION) |
| RA-3 | RA-3 (a) | CCI-001048 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the audit trail of assessments to ensure the organization being inspected/assessed conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction. | [Section 4](#_RISK_ASSESSMENT) |
| RA-3 | RA-3 (b) | CCI-001049 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the risk assessment report to ensure the organization being inspected/assessed documents risk assessment results in the risk assessment report.   DoD has defined the document as a risk assessment report. | [Section 4](#_RISK_ASSESSMENT) |
| RA-3 | RA-3 (b) | CCI-001642 | 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 document as a risk assessment report. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-3 | RA-3 (c) | CCI-001050 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the record of reviews to ensure the organization being inspected/assessed reviews risk assessment results upon re-accreditation.   DoD has defined the frequency as upon re-accreditation. | [Section 4](#_RISK_ASSESSMENT) |
| RA-3 | RA-3 (c) | CCI-001051 | 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 upon re-accreditation. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-3 | RA-3 (d) | CCI-002370 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed disseminates the risk assessment results to the ISSM, ISSO, AO, and PM.   DoD has defined the personnel or roles as the ISSM, ISSO, AO, and PM. | [Section 4](#_RISK_ASSESSMENT) |
| RA-3 | RA-3 (d) | CCI-002371 | 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 the ISSM, ISSO, AO, and PM. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-3 | RA-3 (e ) | CCI-001052 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines historical versions of the risk assessment as well as records of changes to the system to ensure the organization being inspected/assessed updates the risk assessment upon re-accreditation or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.   DoD has defined the frequency as upon re-accreditation. | [Section 4](#_RISK_ASSESSMENT) |
| RA-3 | RA-3 (e ) | CCI-001053 | 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 upon re-accreditation. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 (1) | RA-5 (1) | CCI-001062 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment will:  1. If the inspected organization is using the DoD provided enterprise scanning tool, compliance with this control is complete. 2. Validate the identified tool in use by the inspected organization is able to maintain current up to date information system vulnerability data. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (10) | RA-5 (10) | CCI-002372 | High | High | High | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/ multi-hop attack vectors. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| RA-5 (2) | RA-5 (2) | CCI-001063 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the record of scans to ensure the latest most up to date scanning policies are present. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (2) | RA-5 (2) | CCI-001064 | 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 prior to running scans. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 (3) | RA-5 (3) | CCI-002373 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the organization being inspected/assessed employs the DoD Enterprise scanning tool. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-5 (4) | RA-5 (4) | CCI-001066 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment will review results of validation of base control RA-5, if the inspected organization is compliant with the requirements of RA-5, they are compliant with this control. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (4) | RA-5 (4) | CCI-002374 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented corrective actions to ensure the organization being inspected/assessed defines the corrective actions when information about the information system is discoverable by adversaries.   DoD has determined the corrective actions are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (4) | RA-5 (4) | CCI-002375 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of actions taken to ensure the organization being inspected/assessed takes the corrective actions defined in RA-5 (4), CCI 2374 when information about the information system is discoverable by adversaries. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (5) | RA-5 (5) | CCI-002906 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented vulnerability scanning activities to ensure the organization being inspected/assessed defines the vulnerability scanning activities in which the information system implements privileged access authorization to organization-identified information system components.   DoD has determined the vulnerability scanning activities are not appropriate to define at the Enterprise level. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (5) | RA-5 (5) | CCI-001067 | High Moderate Low | 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 implement privileged access authorization to all information systems and infrastructure components for selected vulnerability scanning activities defined in RA-5 (5), CCI 2906.   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 1067.   DoD has defined the information system components as all information systems and infrastructure components. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 (5) | RA-5 (5) | CCI-001645 | 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 information system components as all information systems and infrastructure components. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 (6) | RA-5 (6) | CCI-001068 | blank | blank | blank | The organization conducting the inspection/assessment validates the organization is employing automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-5 (8) | RA-5 (8) | CCI-001071 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the audit trail to determine if the organization has documented any previously identified exploited vulnerabilities. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-5 | RA-5 (a) | CCI-001054 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results for the 90 days preceding the inspection/assessment.   If the system in question has not been operational for more than 90 days the organization will provide all available scan(s). | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (a) | CCI-001056 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the organization's vulnerability scanning procedures and results in order to validate the organization conducts vulnerability scans of its Information System (IS) and hosted applications when new vulnerabilities potentially affecting the IS and/or applications are identified and reported. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (a) | CCI-001641 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines random vulnerability process documentation (if applicable) to validate the organization has clearly defined and documented a process for conducting random vulnerability scans on the information system and hosted applications.   If the organization being inspected/assessed has determined they have no requirement for random scanning, there is no requirement for a process. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (a) | CCI-001643 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines  the vulnerability scanning results every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs) to verify compliance with the organization being inspected/assessed random vulnerability scanning process.    DoD has defined the frequency as every 30 days or as directed by an authorative source (e.g. IAVM, CTOs, DTMs, STIGs). | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (a) | CCI-001055 | 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 30 days or as directed by an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 | RA-5 (b) | CCI-001057 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the software list or vulnerability scanning procedures to ensure the organization being inspected/assessed employs the DoD Enterprise scanning tool. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (c) | CCI-001058 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment will interview organizational personnel with security control assessment and vulnerability scanning responsibilities. The purpose of the reviews and interviews is to validate the organization is conducting an analysis of the vulnerability scan reports and results from the security control assessments. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (d) | CCI-001059 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines audit records to validate the organization is taking action to remediate legitimate vulnerabilities within the required response times (IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs).   The organization conducting the inspection/assessment may conduct independent vulnerability scans to compare those scan results with audit records of remediation actions.   DoD has defined the response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs, STIGs). | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-5 | RA-5 (d) | CCI-001060 | 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 response times as IAW an authoritative source (e.g. IAVM, CTOs, DTMs). | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 | RA-5 (e ) | CCI-002376 | 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 at a minimum, the ISSO and ISSM. | Automatically compliant with this CCI because they are covered at the DoD level |
| RA-5 | RA-5 (e) | CCI-001061 | High Moderate Low | High Moderate Low | High Moderate Low | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed shares information obtained from the vulnerability scanning process and security control assessments with at a minimum, the ISSM and ISSO to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).     DoD has defined the personnel or roles as at a minimum, the ISSO and ISSM. | [Section 5](#_5.0_VULNERABILITY_SCANNING) |
| RA-6 | RA-6 | CCI-003119 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of surveys to ensure the organization being inspected/assessed employs a technical surveillance countermeasures survey at locations defined in RA-6, CCI 3120 on a frequency defined in RA-6, CCI 3121 or when events or indicators defined in RA-6, CCI 3122 occur. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-6 | RA-6 | CCI-003120 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented locations to ensure the organization being inspected/assessed defines the locations where technical surveillance countermeasures surveys are to be employed.   DoD has determined the locations are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-6 | RA-6 | CCI-003121 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented frequency to ensure the organization being inspected/assessed defines the frequency on which to employ technical surveillance countermeasures surveys.   DoD has determined the frequency is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| RA-6 | RA-6 | CCI-003122 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented events or indicators to ensure the organization being inspected/assessed defines the events or indicators upon which technical surveillance countermeasures surveys are to be employed. | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – RISK ASSESSMENT REPORT TEMPLATE**

This report is focused on risk assessment of non-compliant (NC) security controls and addresses vulnerabilities displayed in the Security Assessment Report (SAR) after the security control assessment has been completed by the Security Control Assessor (SCA). All NC security controls must be subjected to a risk assessment that considers multiple factors in assigning a residual risk level to each NC security control. The individual risk levels are then used to inform the SCA’s recommendation (i.e., SAR executive summary) to the Authorizing Official on acceptance of the cybersecurity risk of operating the system.

