**READ FIRST**

The HACS SOW templates (found on the [HACS website](http://www.gsa.gov/hacs)) provide example information for a variety of cybersecurity services that can be purchased through the HACS Special Item Number (SIN). These templates begin with “Section 3.0 STATEMENT OF WORK” and continue through all of “Section 4.0 DELIVERABLES, INSPECTION, AND ACCEPTANCE.” These sections provide typical language for a cybersecurity solicitation, and provide examples of specific activities and deliverables associated with RMF services.

This template aligns with the HACS Request for Quote (RFQ) Template, and material from this and other SOW examples can be copied and pasted directly into Sections 3.0 and 4.0 of the RFQ template (found on the HACS website) to make your experience easier and more efficient. These templates provide prompts for agencies to input their specific information in <red text>. While these templates provide information on cybersecurity services, agencies should make sure that solicitations contain the specific requirements of their organization.

**(SAMPLE RFQ LANGUAGE IS IN RED)**

[DISCLAIMER: The language contained herein is just a sample of what can be used. There is no requirement or expectation that agencies use the same language in RFQs.]

# 

# 3.0 STATEMENT OF WORK (SOW)

# 3.1 OVERVIEW AND BACKGROUND

The Risk Management Framework (RMF) provides a common information security framework for the Federal Government including the Department of Defense (DoD) and the Intelligence Community (IC). It is based on publications by the National Institute of Standards and Technology (NIST) and the Committee on National Security Systems (CNSS). The RMF is integral to the implementation of the Federal Information Security Modernization Act (2014).

The RMF, which is explained in NIST SP 800-37, Rev. 2, provides a structured approach to integrate risk management and information security into the System Development Lifecycle (SDLC) process. The seven steps of the RMF include preparation, security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The RMF promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of continuous monitoring processes; provides senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions; and integrates information security into the enterprise architecture and system development life cycle.

<Insert agency name> <describe organization and outline specific departments or systems included for this RFQ>

# 3.2 OBJECTIVE

This RFQ seeks contractors awarded the HACS SIN under the Multiple Award Schedule Information Technology (MAS IT). Additionally, the contractor must be cataloged in either of the following subcategories under SIN 54151HACS.

* High Value Asset (HVA) Assessment
* Risk and Vulnerability Assessment (RVA)

The contract shall be for non-personal services to provide RMF services on <Insert agency name and system name>. The contractor shall provide all personnel and items necessary to perform the functional and technical support described in this SOW, except those items specified as Government furnished equipment/property. The contractor shall perform all tasks identified in this SOW.

# 3.3 SCOPE

The scope of this cybersecurity services contract for <Insert agency name and system name> includes the following:

* <Insert scope of services required>

**3.4 REFERENCES**

The contractor shall be familiar with Federal policies, program standards, and guidelines such as, but not limited to, those listed below or later versions as applicable:

| **REFERENCE** | **DESCRIPTION / TITLE** |
| --- | --- |
| **FISMA** | *Federal Information System Modernization Act (FISMA) (2014)* |
| **FIPS 199** | *Federal Information Processing Standards (FIPS) Publication 199 - Standards for Security Categorization of Federal Information and Information Systems* |
| **FIPS 200** | *Minimum Security Requirements for Federal Information and Information Systems* |
| **NIST SP 800-30 Rev 1** | *National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments* |
| **NIST SP 800-35** | *Guide to Information Technology Security Services* |
| **NIST SP 800-37 Rev 2** | *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* |
| **NIST SP 800-39** | *Managing Information Security Risk: Organization, Mission, and Information System View* |
| **NIST SP 800-44 Version 2** | *Guidelines on Securing Public Web Servers* |
| **NIST SP 800-53 Rev 4** | *Security and Privacy Controls for Federal Information Systems and Organizations* |
| **NIST SP 800-53A Rev 4** | *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* |
| **NIST SP 800-61 Rev 2** | *Computer Security Incident Handling Guide* |
| **NIST SP 800-83 Rev 1** | *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* |
| **NIST SP 800-86** | *Guide to Integrating Forensic Techniques into Incident Response* |
| **NIST SP 800-101 Rev 1** | *Guidelines on Mobile Device Forensics* |
| **NIST SP 800-115** | *Technical Guide to Information Security Testing and Assessment* |
| **NIST SP 800-128** | *Guide for Security-Focused Configuration Management of Information Systems* |
| **NIST SP 800-137** | *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* |
| **NIST SP 800-150** | *Guide to Cyber Threat Information Sharing* |
| **NIST SP 800-153** | *Guidelines for Securing Wireless Local Area Networks (WLANs)* |
| **NIST SP 800-160 Vol 1** | *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* |
| **NIST SP 800-171** **Rev 1** | *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* |
| **NIST SP 800-171A** | *Assessing Security Requirements for Controlled Unclassified Information* |
| **NIST SP 800-181** | *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* |
| **P.L. 93-579** | *Public Law 93-579 Privacy Act, December 1974 (Privacy Act)* |
| **40 U.S.C. 11331** | *Responsibilities for Federal Information Systems Standards* |
| **OMB M-19-03** | *Office of Management and Budget (OMB) Memorandum 19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* |
| **OMB A-130** | *OMB Circular A-130, Managing Information as a Strategic Resource* |
| **BOD 18-02** | *Department of Homeland Security’s Binding Operational Directive 18-02, Securing High Value Assets* |
| **<Add as needed>** |  |

# 3.5 REQUIREMENTS/TASKS

[The following tasks provide example RMF activities. Adjust these tasks to align with your specific requirements and with additional guidance from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and NIST.]

The contractor shall provide the knowledge, skills, abilities, staff support, and other related resources necessary to conduct the following RMF related services:

* *Prepare*
* *Categorize* Information Systems
* *Select* Security Controls
* *Implement* Security Controls
* *Assess* Security Controls
* *Authorize* Information System
* *Monitor* Security Controls
* Other RMF Related Services

The contractor shall follow the issue resolution process for any identified vulnerability or issue identified throughout the RMF. Issue resolution is used to communicate issues to key stakeholders and document risk-based decisions to include risk acceptance, correcting vulnerabilities and retesting, or creating a Plan of Action and Milestones (POA&M). Issue resolution provides an audit trail, accelerates the RMF, and documents management accountability.

# 3.5.1 PREPARE

Carry out activities at the organization, mission, business process, and information system levels of the enterprise to help prepare the <Insert agency name> to manage its security and privacy risks using the RMF. During the Prepare step the contractor shall assist in the following activities <agencies should pick from the following list of Prepare activities that they would like a contractor involved in>:

* Determine and assign roles to risk management resources
* Develop a risk management strategy for the organization that includes a determination and expression of organizational risk tolerance
* Perform an organization-wide risk assessment
* Establish and document organizationally-tailored control baselines
* Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems
* Develop and implement an organization-wide strategy for continuously monitoring control effectiveness
* Identify and document assets that require protection
* Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis
* Define and document the security and privacy requirements for the system and the environment of operation
* Determine the placement of the system within the enterprise architecture

# 

# 3.5.2 CATEGORIZE INFORMATION SYSTEMS

Categorize the information system into low, moderate, or high potential security impact, using FIPS 199 as a guide. Use NIST 800-60 Volume 2 to determine the security categorization of the system based on the organization’s requirements. The results of the security categorization should be documented in the security plan. This task consists of the following subtasks:

* Subtask 1 - Security Categorization
* Subtask 2 - Information System Description
* Subtask 3 - Information System Registration

# 3.5.2.1 Subtask 1 - Security Categorization

The contractor shall categorize the information system and document the results of the security categorization in the Security Plan. Deliverables for Security Categorization include, but are not limited to, a written subsection of the System Security Plan that covers FIPS 199 Standards for Security Categorization of Federal Information and Information Systems.

# 3.5.2.2 Subtask 2 - Information System Description

The contractor shall describe the information system (including system boundary) and document the description in the Security Plan. Deliverables for Information System Description include, but are not limited to, a written System Definition Document which is a subsection in the System Security Plan.

**3.5.2.3 Subtask 3 - Information System Registration**

The contractor shall register the information system with appropriate organizational

program/management offices. <Insert agency specific deliverables for Information System Registration here and in the deliverable table in section 4.3>.

# 3.5.3 SELECT SECURITY CONTROLS

Select Security Controls using FIPS 200 as a guide which specifies the minimum security requirements for federal information systems or NIST SP 800-53 to establish a minimum/baseline controls set based on the security level determination of the information system. The selected controls should be documented in the security control section of the System Security Plan. This task consists of the following subtasks:

* Subtask 1 - Common Control Identification
* Subtask 2 - Security Control Selection
* Subtask 3 - Monitoring Strategy
* Subtask 4 - Security Plan Approval

**3.5.3.1 Subtask 1 - Common Control Identification**

The contractor shall identify the security controls that are provided by the organization

as common controls for organizational information systems and document the controls

in the Security Plan (or equivalent document). Deliverables for Common Control

Identification include, but are not limited to, a Security Control Selection Document

included in the System Security Plan.

**3.5.3.2 Subtask 2 - Security Control Selection**

The contractor shall select the security controls for the information system and document the controls in the Security Plan. Deliverables for Security Control Selection include, but are not limited to, Updated Security Control Selection Documentation.

**3.5.3.3 Subtask 3 - Monitoring Strategy**

The contractor shall develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation. Deliverables for Monitoring Strategy include, but are not limited to, a Monitoring Strategy Document and a Briefing (slides and meeting support).

**3.5.3.4 Subtask 4 - Security Plan Approval**

The contractor shall request Government review and approval of the Security Plan. Deliverables for Security Plan Approval include, but are not limited to, a Security Plan Approval Recommendation Letter.

# 3.5.4 IMPLEMENT SECURITY CONTROLS

Implement the security controls specified in the Security Plan. As appropriate, document the security control implementation and contingency plan in the System Security Plan, providing a functional description of the control implementation. Ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies. This task consists of the following subtasks:

* Subtask 1 - Security Control Implementation
* Subtask 2 - Security Control Documentation

**3.5.4.1 Subtask 1 - Security Control Implementation**

The contractor shall implement the security controls specified in the security control selection document or identified in the System Security Plan, and develop an implementation status report. Deliverables for Security Control Implementation include, but are not limited to, an Implementation Status Report.

**3.5.4.2 Subtask 2 - Security Control Documentation**

The contractor shall document the security control implementation, as appropriate, in the Security Plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). Deliverables for Security Control Documentation include, but are not limited to, an Updated System Security Plan.

# 3.5.5 ASSESS SECURITY CONTROLS

Create the Security Assessment Plan (SAP) to document the assessment schedule, tools, and personnel. Approval of the assessment approach and scope should be obtained. A Rules of Engagement (ROE) document should be developed where vulnerability scanning or penetration testing procedures are included in the assessment. A final report of the assessment findings should be documented in the Security Assessment Report (SAR). This task consists of the following subtasks:

* Subtask 1 - Assessment Preparation
* Subtask 2 - Security Control Assessment
* Subtask 3 - SAR
* Subtask 4 - Remediation Actions

# 

# 3.5.5.1 Subtask 1 - Assessment Preparation

The contractor shall develop, review, and obtain Government approval of a plan to assess the security controls, and develop a ROE document. Deliverables for Assessment Preparation include a SAP and ROE.

# 3.5.5.2 Subtask 2 - Security Control Assessment

The contractor shall assess the security controls in accordance with the assessment procedures defined in the SAP. Deliverables for Security Control Assessment include, but are not limited to, a Security Categorization Review, a System Security Plan Analysis, and a Security Assessment.

# 3.5.5.3 Subtask 3 - Security Assessment Report (SAR)

The contractor shall prepare the SAR documenting the issues, findings, and recommendations from the security control assessment. Deliverables for SAR include, but are not limited to, an SAR that includes a Vulnerability Assessment and a Briefing (slides and meeting support).

# 3.5.5.4 Subtask 4 - Remediation Actions

The contractor shall conduct initial remediation actions based on the findings and recommendations of the SAR. Deliverables for Remediation Actions include, but are not limited to, an Issue Resolution Report and a Remediation Status Report.

# 3.5.6 AUTHORIZE INFORMATION SYSTEM

The system Authorizing Official signs the system Authorization to Operate (ATO) based on the risk level of the system reported in the SAR, as well as the POA&M, created to correct audit findings and the completion of the Assessment and Authorization (A&A) Package. This task consists of the following subtasks:

* Subtask 1 - POA&M
* Subtask 2 - Security Authorization Package
* Subtask 3 - Risk Determination
* Subtask 4 - Risk Acceptance

# 3.5.6.1 Subtask 1 - Plan of Action and Milestones (POA&M)

The contractor shall prepare the POA&M, consisting of tasks needing to be accomplished and schedules to remediate system weaknesses, based on the findings and recommendations of the SAR excluding any remediation actions taken. Deliverables for the POA&M include, but are not limited to, a POA&M Tracker.

# 3.5.6.2 Subtask 2 - Security Authorization Package

The contractor shall assemble the security authorization package, containing the results of the SAR, the POA&M, the System Security Plan, and other documents that provide the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation. The package is submitted to the authorizing official for adjudication. The deliverable for this subtask includes, but is not limited to, a Security Authorization Package.

# 3.5.6.3 Subtask 3 - Risk Determination

The contractor shall determine the risk (including risk to mission, functions, image, or reputation) to organizational operations, organizational assets, individuals, other organizations, or the Nation. Deliverables for risk determination include, but are not limited to, a Residual Risk Statement that will be included in the Risk Acceptance Recommendation Report, and a Briefing (slides and meeting support).

# 3.5.6.4 Subtask 4 - Risk Acceptance

The contractor shall determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. Deliverables for Risk Acceptance include, but are not limited to, a Risk Acceptance Recommendation Report and a Briefing (slides and meeting support).

# 3.5.7 MONITOR SECURITY CONTROLS

Continuously monitor where NIST 800-137 is used as a guide, and test a portion of the applicable security controls annually. Perform periodic vulnerability scanning and security impact analysis of changes. This task consists of the following subtasks:

* Subtask 1 - Information System and Environment Changes
* Subtask 2 - Ongoing Security Control Assessment
* Subtask 3 - Ongoing Remediation Actions
* Subtask 4 - Key Updates
* Subtask 5 - Security Status Reporting
* Subtask 6 - Ongoing Risk Determination and Acceptance

# 3.5.7.1 Subtask 1 - Information System and Environment

# Changes

The contractor shall determine and document the security impact of proposed or actual changes to the information system and its environment of operation. Deliverables for Information System and Environment Changes include, but are not limited to, an Impact Assessment Report.

# 3.5.7.2 Subtask 2 - Ongoing Security Control Assessment

The contractor shall assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy. Deliverables for Ongoing Security Control Assessment include, but are not limited to, an updated Residual Risk Statement and an updated SAR.

# 3.5.7.3 Subtask 3 - Ongoing Remediation Actions

The contractor shall conduct selected remediation actions based on the results of ongoing monitoring activities and the outstanding items in the POA&M. Deliverables for Ongoing Remediation Actions include, but are not limited to, an updated Issue Resolution Report and an updated Remediation Status Report.

# 

# 3.5.7.4 Subtask 4 - Key Updates

The contractor shall update the Security Plan, SAR, and POA&M based on the results of the continuous monitoring process. Deliverables for Key Updates include, but are not limited to, an updated Residual Risk Statement and an updated Risk Acceptance Recommendation Report.

# 3.5.7.5 Subtask 5 - Security Status Reporting

The contractor shall report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system), to appropriate organizational officials on an ongoing basis in accordance with the organization-defined monitoring strategy. Deliverables for Security Status Reporting include, but are not limited to, daily, weekly, and/or monthly Status Reports and Documentation, as required.

# 3.5.7.6 Subtask 6 - Ongoing Risk Determination and

# Acceptance

The contractor shall review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable. Deliverables for Ongoing Risk Determination and Acceptance include, but are not limited to, an updated Residual Risk Statement, and an updated Risk acceptance Recommendation Report.

**3.5.8 OTHER RMF RELATED SERVICES**

Any task performed and documented to supplement the RMF in order for the organization’s system to attain an ATO would be considered other RMF related services. These services are implemented contingent upon the security requirements of the system being assessed. This task consists of the following subtasks:

* Subtask 1 - Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA)
* Subtask 2 - Information System Removal and Decommissioning
* Subtask 3 - Incident Response Plan and Procedure
* Subtask 4 - Updated Risk Assessment

**3.5.8.1 Subtask 1 - Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA)**

The contractor shall prepare for and develop interconnection documentation

identify stakeholders, ensure proper documentation is completed, and help develop the MOU and the ISA. The MOU contains the responsibilities between parties with system connection while the ISA supports the MOU by specifying technical details of the connection. These documents should be included in the final A&A package if applicable. Deliverables for MOU and ISA include, but are not limited to, a MOU and an ISA.

**3.5.8.2 Subtask 2 - Information System Removal and**

**Decommissioning**

The contractor shall request and review existing system security documentation and meet with key stakeholders to determine the level of effort and resources required to complete the decommissioning. Deliverables for Information System Removal and Decommissioning include, but are not limited to, a Decommissioning Plan, tracking and management system information, a Decommissioning Security Status Report, and an Impact Assessment Report.

**3.5.8.3 Subtask 3 - Incident Response Plan and Procedure**

The contractor shall request and review incident response plan policy and procedures and existing system security documentation and develop incident response strategies and procedures. Deliverables for Incident Response Plan and Procedure include, but are not limited to, an Incident Response Plan and Procedures Document.

**3.5.8.4 Subtask 4 - Updated Risk Assessment**

The contractor shall discuss and record potential threats (human intentional/unintentional, natural, and environmental), flaws, weaknesses, and existing security controls of the information system. Deliverables for Updated Risk Assessment include, but are not limited to, updated Risk Assessment Documentation.

**(SAMPLE RFQ LANGUAGE IS IN RED)**

[DISCLAIMER: The language contained herein is just a sample of what can be used. There is no requirement or expectation that agencies use the same language in RFQs.]

**4.0 DELIVERABLES, INSPECTION, AND ACCEPTANCE**

# 4.1 SCOPE OF INSPECTION

All deliverables will be inspected by the Contracting Officer’s Representative (COR) for content, completeness, accuracy, and

conformance under this agreement and the specifics of the project.

## 4.2 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the SOW, the contractor's quote, and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable provisions.

1. Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.
2. If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.
3. All of the Government's comments to deliverables must either be incorporated in the succeeding version or the contractor must demonstrate, to the Government's satisfaction, why such comments should not be incorporated.
4. If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this contract, the document may be immediately rejected without further review and returned to the contractor for correction and re-submission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

## 4.3 DRAFT AND FINAL DELIVERABLES

All written deliverables require at least two iterations – a draft and a final. The final document must be approved and accepted by the Government prior to payment submission. The contractor shall submit draft and final documents, using <Microsoft Office 2010/add or replace as applicable> or later, to the Government electronically. The Government requires <insert number> business days for review and submission of written comments to the contractor on draft and final documents. The contractor shall make revisions to the deliverables and incorporate the Government’s comments into draft and final deliverables before submission. Upon receipt of the Government’s comments, the contractor shall have <insert number> business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

Any issues that cannot be resolved by the contractor in a timely manner shall be identified and referred to the COR.

The COR is designated by the Contracting Officer (CO) to perform as the technical liaison between the contractor’s management and the CO in routine technical matters constituting general program direction within the scope of the contract. Under no circumstances is the COR authorized to affect any changes in the work required under the contract, or enter into any agreement that has the effect of changing the terms and conditions of the contract or that causes the contractor to incur any costs. In addition, the COR will not supervise, direct, or control contractor employees.

Notwithstanding this provision, to the extent the contractor accepts any direction that constitutes a change to the contract without prior written authorization of the CO, costs incurred in connection therewith are incurred at the sole risk of the contractor, and if invoiced under the contract, will be disallowed. On all matters that pertain to the contract/contract terms, the contractor must communicate with the CO.

Whenever, in the opinion of the contractor, the COR requests efforts beyond the terms of the contract, the contractor shall so advise the CO. If the COR persists and there still exists a disagreement as to proper contractual coverage, the CO shall be notified immediately, preferably in writing. Proceeding with work without proper contractual coverage may result in nonpayment or necessitate submission of a claim.

**SAMPLE LIST OF DELIVERABLES**

| **DELIVERABLE** | **SOW  REFERENCE** | **DELIVERY  DATE** |
| --- | --- | --- |
| Project Management Plans | Insert related SOW reference | No Later Than (NLT) <insert number of days> business days after task assignment |
| Organizational Conflict of Interest Plan | Insert related SOW reference | NLT <insert number of days> business days after award |
| Meeting Briefings/Presentations | Insert related SOW reference | NLT <insert number of days> business days prior to scheduled meeting |
| Rules of Engagement | Insert related SOW reference | NLT <insert number of days> business days after award |
| Status Reports | Insert related SOW reference | NLT the 15th of each month |
| System Security Plan subsection that covers FIPS 199 Standards for Security Categorization of Federal Information and Information Systems | 3.5.2.1 | NLT <insert number of days> business days after task assignment |
| System Definition Document | 3.5.2.2 | NLT <insert number of days> business days after award |
| Security Control Selection Document | 3.5.3.1 | NLT <insert number of days> business days prior to scheduled meeting |
| Updated Security Control Selection Documentation | 3.5.3.2 | NLT <insert number of days> business days after award |
| Monitoring Strategy Document and Briefing | 3.5.3.3 | NLT <insert number of days> business days after award |
| Security Plan Approval Recommendation Letter | 3.5.3.4 | NLT <insert number of days> business days after task assignment |
| Implementation Status Report | 3.5.4.1 | NLT <insert number of days> business days after task assignment |
| Updated System Security Plan | 3.5.4.2 | NLT <insert number of days> business days after task assignment |
| Rules of Engagement | 3.5.5.1 | NLT <insert number of days> business days after task assignment |
| Security Categorization Review | 3.5.5.2 | NLT <insert number of days> business days after task assignment |
| System Security Plan Analysis | 3.5.5.2 | NLT <insert number of days> business days after task assignment |
| Security Assessment | 3.5.5.2 | NLT <insert number of days> business days after task assignment |
| SAR that includes a Vulnerability Assessment and Briefing | 3.5.5.3 | NLT <insert number of days> business days after task assignment |
| Issue Resolution Report, Remediation Status Report | 3.5.5.4 | NLT <insert number of days> business days after task assignment |
| POA&M Tracker | 3.5.6.1 | NLT <insert number of days> business days after task assignment |
| Security Authorization Package | 3.5.6.2 | NLT <insert number of days> business days after task assignment |
| Residual Risk Statement, to be included in the Risk Acceptance Recommendation Report and Briefing | 3.5.6.3 | NLT <insert number of days> business days after task assignment |
| Risk Acceptance Recommendation Report and Briefing | 3.5.6.4 | NLT <insert number of days> business days after task assignment |
| Impact Assessment Report | 3.5.7.1 | NLT <insert number of days> business days after task assignment |
| Updated SAR | 3.5.7.2 | NLT <insert number of days> business days after task assignment |
| Updated Issue Resolution Report | 3.5.7.3 | NLT <insert number of days> business days after task assignment |
| Updated Remediation Status Report | 3.5.7.3 | NLT <insert number of days> business days after task assignment |
| Updated Risk Acceptance Recommendation Report | 3.5.7.4 | NLT <insert number of days> business days after task assignment |
| Daily, Weekly, and/or Monthly Status Reports and Documentation | 3.5.7.5 | NLT <insert number of days> business days after task assignment |
| Updated Risk Acceptance Recommendation Report | 3.5.7.6 | NLT <insert number of days> business days after task assignment |
| MOU | 3.5.8.1 | NLT <insert number of days> business days after task assignment |
| ISA | 3.5.8.1 | NLT <insert number of days> business days after task assignment |
| Decommissioning Plan | 3.5.8.2 | NLT <insert number of days> business days after task assignment |
| Decommissioning Security Status Report | 3.5.8.2 | NLT <insert number of days> business days after task assignment |
| Impact Assessment Report | 3.5.8.2 | NLT <insert number of days> business days after task assignment |
| Incident Response Plan and Procedures Document | 3.5.8.3 | NLT <insert number of days> business days after task assignment |
| Updated Risk Assessment Documentation | 3.5.8.4 | NLT <insert number of days> business days after task assignment |

## 4.4 NON-CONFORMING DELIVERABLES

Non-conforming products or services will be rejected. Deficiencies will be corrected by the contractor within <insert number of days> business days of the rejection notice. If the deficiencies cannot be corrected within <insert number of days> business days, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within <insert number of days> business days.