**READ FIRST**

The Application Security Testing (AST) Statement of (SOW) template provides sample information for a variety of cybersecurity services that can be purchased relative to an application security testing program. This template begins with “Section 3.0 STATEMENT OF WORK” and continues through “Section 4.0 DELIVERABLES, INSPECTION, AND ACCEPTANCE.” These sections provide typical language for a cybersecurity solicitation and examples of specific activities and deliverables including services requirements.

This template aligns with the Highly Adaptive Cybersecurity Services (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 HACS RFQ Template to make your experience easier and more efficient. These templates provide prompts, in <red text>, for agencies to input their specific information. While these templates provide information on generalized cybersecurity services, agencies should make sure that solicitations contain their agency specific requirements and adhere to any agency specific procurement guidelines.

**(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 Office of Management and Budget (OMB) Memorandum M-22-09 “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” describes five (5) complementary areas of effort (pillars): Identity, Devices, Networks, Applications and Workloads, and Data. Under the Applications and Workloads pillar, the memo outlines six (6) actions Federal agencies need to take to improve application security. Specifically, agencies must operate dedicated Application Security Testing (AST) programs and utilize high-quality firms specializing in application security for independent third-party evaluation.

AST is the process of testing, analyzing, and reporting on the security level of an application as it moves through the Software Development Life Cycle (SDLC). AST makes applications more resistant to security threats by identifying poor coding practices that lead to logic flaws and path traversal security weaknesses and vulnerabilities in the source code.

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

##

## 3.2 OBJECTIVE

This SOW describes the requirements for the GSA RFQ <RFQ number>, which seeks contractors holding a GSA Multiple Award Schedule Information Technology (MAS IT) Category contract.

The contract shall be for non-personal services to provide AST 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 based on the specified organization’s risk management strategy. The contractor shall support in performing test planning with respect to identifying and documenting the resources, schedule, risks, and methodologies that shall be used during testing and documenting the test planning efforts. The contractor will undertake all the necessary tasks to help the organization to meet business requirements for confidentiality, integrity, and availability of its application.

##

## 3.3 SCOPE

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

● <Insert scope of services required>

* Testing Plan/Design/Updates/Reporting
* Software Development Testing
* Software Pre-release Testing
* Software Deployment Testing

### Red Team Application Security Exercises

.

## 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 amended:

| **REFERENCE** | **DESCRIPTION / TITLE** |
| --- | --- |
| 40 U.S.C. 11331 | U.S. Code (U.S.C.) 11331, Responsibilities for Federal Information Systems Standards |
| BOD 18-02 | Department of Homeland Security’s Binding Operational Directive (BOD) 18-02, Securing High Value Assets |
| BOD 20-01 | Develop and Publish a Vulnerability Disclosure Policy |
| E.O. 14028 | Executive Order (E.O.) 14028 Improving the Nation’s Cybersecurity |
| 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 |
| FISMA | Federal Information System Modernization Act (FISMA) (2014) |
| NIST IR 8018 | NIST Internal Report (IR) 8018, Public Safety Mobile Application Security Requirements Workshop Summary |
| NIST IR 8135 | Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report |
| NIST IR 8397 | Guidelines on Minimum Standards for Developer Verification of Software |
| NIST SP 500-268 | NIST Special Publication (SP) 500-268, Source Code Security Analysis Tool Function Specification Version 1.1 |
| NIST SP 500-269 | Software Assurance Tools: Web Application Security Scanner Functional Specification Version 1.0 |
| NIST SP 500-270 | Source Code Security Analysis Tool Test Plan Version 1.1 |
| NIST SP 800-30 Rev 1 | 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 Ver 2 | Guidelines on Securing Public Web Servers |
| NIST SP 800-53 Rev 5 | Security and Privacy Controls for Information Systems and Organizations |
| NIST SP 800-53A Rev 5 | Assessing Security and Privacy Controls in Information Systems and Organizations |
| 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 800-161 Rev 1 | Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations |
| NIST SP 800-163 Rev 1 | Vetting the Security of Mobile Applications |
| NIST SP 800-218 | Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities |
| NIST Project | NIST Software Assurance Metrics and Tool Evaluation (SAMATE) Project |
| OMB A-130 | Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource |
| OMB M-19-03 | OMB Memorandum (M-19-03) Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program |
| OMB M-20-32 | Improving Vulnerability Identification, Management, and Remediation |
| OMB M-21-30 | Protecting Critical Software Through Enhanced Security Measures |
| OMB M-22-09 | Moving the U.S. Government Toward Zero Trust Cybersecurity Principles |
| OMB M-22-18 | Enhancing the Security of Software Supply Chain Through Secure Software Development Practices |

## 3.5 REQUIREMENTS / TASKS

[The following tasks provide sample activities for example activities for AST services. Adjust these tasks to align with your agency specific requirements and with additional guidance from the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST).]

The contractor may propose an optimal workflow and labor mix. Deployment to production servers will be made in coordination with <insert organization name> technical staff.

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

* Testing Plan/Design/Updates
* Software Development Testing
* Software Pre-release Testing
* Software Deployment Testing

### Red Team Application Security Exercises

Knowledge and skills required for AST methodologies include, but are not limited to:

* Knowledge of Agile Security Testing, Open Web Application Security Project® (OWASP) Security Testing Framework, OWASP Code Review Guide, Penetration Testing Methodologies and Standards, Information System Security Assessment Framework, Open-Source Security Testing Methodology Manual, Building Security in Maturity Model.

###

### 3.5.1 Testing Plan / Design / Updates

### 3.5.1.1 Test Planning

### The contractor will create a test plan which outlines the strategy that will be used to test an application, resources that will be used, test environment in which testing will be performed, limitations of the testing, and schedule of the testing activities. Before the start of a security test, detailed guidelines and constraints regarding the execution of the test must be agreed upon and approved by the agency's stakeholders (e.g., Information Systems Security Officer or System Owner) in a signed document. This approval grants the contractor authority to conduct the defined activities.

### 3.5.1.2 Test and Deploy Application Updates

The contractor shall coordinate application testing activities with each application update. Deployment to production servers will be made in coordination with <insert organization name> technical staff.

The contractor shall create a security impact analysis for application releases prior to changes going live into a production environment.

###

### 3.5.1.3 Application Threat Modeling

Once the contractor finishes the kick-off meeting with the organization, the contractor will prepare application threat modeling documentation for <Insert agency name and system name> to identify, quantify, and address security risks before starting testing activities.

###

### The contractor shall implement a structured application threat modeling approach that addresses the security risks associated with an application.

###

### To support the application threat modeling task, the contractor shall:

* Create and/or Update the Application Threat Modeling Standard Operating Procedure (SOP) to identify, quantify and address security risks early in application development. The procedures shall document the implementation of a structured application threat modeling approach to complement static code reviews. The SOP shall include, at a minimum, the following:
	+ Assessment Scope
	+ System Modeling
	+ Threat Identification
	+ Vulnerability Identification
	+ Examination of the Threat History
	+ Evaluation or Impact on the Business
	+ Identification of Integrated Development Environments of security risk awareness
	+ Identification of security coding standards and code review processes
* Create and/or update the Application Threat Modeling Implementation Plan to integrate into the <Insert agency name> SDLC. The implementation plan shall include, at a minimum, the following:
	+ Major milestones
	+ Dependencies
	+ Overall timeline for integration
* Create and/or update the Security Threat Response Plan that identifies countermeasures to reduce the risk to acceptable levels.

### 3.5.2 Software Development Testing

###

### 3.5.2.1 Static Application Security Testing (SAST) in Development Phase

SAST reviews static analysis scan results in real-time and detects security vulnerabilities within the source, binary, or byte code of applications.

The contractor shall scan an application’s source code during development to detect security vulnerabilities.

The contractor shall provide a Static Application Security Testing Report that lists any identified security vulnerabilities, including the type of vulnerability and the vulnerability location in the application’s codebase.

**3.5.2.2 Software Composition Analysis (SCA)**

The contractor shall identify open-source software (OSS) in a codebase, for the purpose of risk management, security, and license compliance.

The agency will provide an application Software Bill of Materials (SBOM). The contractor shall provide a full accounting of the open source and third-party components used in the SBOM application.

**3.5.2.3 Remediation Validation in Development Phase**

No sooner than <insert number of business days> business days and no later than <insert number of business days> business days of the acceptance of any test report, the contractor shall validate that any vulnerabilities identified in the test report during the development phase have been remediated.

The contractor shall provide a Remediation Validation Report that lists any previously-identified vulnerabilities and whether or not they have been remediated.

### 3.5.3 Software Pre-release Testing

### 3.5.3.1 Application Penetration Testing in Pre-release Phase

The contractor shall provide both internal and external security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application.

The contractor shall follow a well-developed and proven methodology to conduct a penetration testing assessment of the target application and supporting services from both an unauthorized/unauthenticated and authorized/authenticated users’ perspective to determine any vulnerabilities that are accessible to an attacker.

During each assessment, the contractor shall also identify common security vulnerabilities, including but not limited to information leakage, Structured Query Language (SQL) injection, and cross-site request forgery.

Deliverables for Penetration Testing include, but are not limited to:

* Rules of Engagement document containing the type and scope of testing, and client contact details
* Penetration Test Report that includes an executive summary, a contextualized walkthrough of technical risks, potential impact of vulnerabilities found, and vulnerability remediation options.
	+ - The contractor shall keep all information pertaining to the applications being tested and other information provided and / or captured during each assessment encrypted manner with no public access.
		- All data will be kept for a period of time agreed upon between <Insert agency name> and the contractor, after which the data shall be destroyed in a secure manner in accordance with policy and standards for destruction of digital data.

####

#### 3.5.3.1.1 Web Application Intrusion Test in Pre-release Phase

<Insert agency name and system name> will give all the necessary information about its website, including URLs and different accounts credentials, to the contractor in charge of the penetration tests. The contractor will try to compromise and exploit the vulnerabilities found during the intrusion tests.

The contractor shall simulate attacks of the agency’s system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure.

Deliverables for Web Application Intrusion Testing include, but are not limited to:

* Rules of Engagement document containing the type and scope of testing, and client contact details
* Web Application Intrusion Test Report that includes an executive summary, methodology and goals, scenario and scope, attack narrative, observations and recommendations, and a conclusion.
	+ - The contractor shall keep all information pertaining to the applications being tested and other information provided and / or captured during each assessment encrypted manner with no public access.
		- All data will be kept for a period of time agreed upon between <Insert agency name> and the contractor, after which the data shall be destroyed in a secure manner in accordance with policy and standards for destruction of digital data.

### 3.5.3.2 Web Application Assessment

Web Application Assessment identifies application vulnerabilities to gain actionable recommendations for remediation. It utilizes a combination of dynamic scanners, open source tools / scripts, and manual testing to test the integrity of the application.

The contractor shall conduct a Web Application Assessment that includes scanning, testing, or both of outward facing web applications for defects in web service implementation that may lead to exploitable vulnerabilities.

The contractor shall provide a Web Application Assessment Report that indicates whether traditional network security tools and techniques are used to limit access to the web service to only those networks and systems that should have legitimate access.

#### 3.5.3.3 Mobile Application Security Testing (MAST) in Pre-release Phase

#### MAST analyzes and identifies vulnerabilities in applications used with mobile platforms (e.g., iOS, Android, and Windows 10 Mobile) and identifies critical information exposures attributed to mobile applications in the environment.

####

#### The contractor shall analyze the security posture of new mobile technologies in development and identify critical information exposure and vulnerabilities attributed to mobile applications used with mobile platforms.

####

#### The contractor shall provide a Mobile Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

####

#### 3.5.3.4 Static Application Security Testing (SAST) in Pre-release Phase

SAST reviews static analysis scan results in real-time and detects security vulnerabilities within the source, binary, or byte code of applications.

The contractor shall scan an application’s source code during pre-release to detect security vulnerabilities.

The contractor shall provide a Static Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

**3.5.3.5 Dynamic Application Security Testing (DAST) in Pre-release Phase**

DAST simulates controlled attacks on a running application or service to identify exploitable vulnerabilities in a running environment with no access to the application source code architecture.

The contractor shall conduct tests to find security vulnerabilities in applications while the application is running, verifying the security during run time by testing different attack types against the running application.

The contractor shall provide a Dynamic Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

**3.5.3.6 Manual Testing in Pre-release Phase**

The primary goal of manual security testing is to perform secure code review to discover flaws, errors, or weaknesses that lead to vulnerabilities in an application that might not be easily revealed by automated security testing alone.

The contractor shall manually test the application by executing test cases using secure code review, perform expert analysis on findings, and generate test reports without the aid of any automated AST tools.

The contractor shall provide a Test Report with an executive summary, detailed findings, and vulnerability risk analysis in the context of the application hosting environment and the agency’s mission and functions.

The contractor shall develop a Remediation Plan for found vulnerabilities. The plan will consist of the following:

* Detailed list of vulnerability findings
* Vulnerability findings prioritized by risk level
* Implementation Plan for fix / patches of vulnerabilities
* Plan for monitoring reliability of fixes

The agency will remediate vulnerabilities according to the Remediation Plan and the contractor shall validate remediated vulnerabilities by re-testing.

#### 3.5.3.7 Remediation Validation in Pre-Release Phase

No sooner than <insert number of business days> business days and no later than <insert number of business days> business days of the acceptance of any test report, the contractor shall validate that any vulnerabilities identified in the test report during the pre-release phase have been remediated by the agency.

The contractor shall provide a Remediation Validation Report that lists any previously-identified vulnerabilities and whether or not they have been remediated.

###

### 3.5.4 Software Deployment Testing

#### 3.5.4.1 Application Penetration Testing in Development Phase

The contractor shall provide both internal and external security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application.

The contractor shall follow a well-developed and proven methodology to conduct a penetration testing assessment of the target application and supporting services from both an unauthorized/unauthenticated and authorized/authenticated users’ perspective to determine any vulnerabilities that are accessible to an attacker.

During each assessment, the contractor shall identify common security vulnerabilities, including but not limited to information leakage, SQL injection, and cross-site request forgery.

Deliverables for Penetration Testing include, but are not limited to:

* Rules of Engagement document containing the type and scope of testing, and client contact details.
* Penetration Test Report that includes an executive summary, a contextualized walkthrough of technical risks, potential impact of vulnerabilities found, and vulnerability remediation options.
	+ - The contractor shall keep all information pertaining to the applications being tested and other information provided and/or captured during each assessment encrypted manner with no public access.
		- All data will be kept for a period of time agreed upon between <Insert agency name> and the contractor, after which the data shall be destroyed in a secure manner in accordance with policy and standards for destruction of digital data.

###

#### 3.5.4.1.1 Web Application Intrusion Test

<Insert agency name and system name> will give all the necessary information about its website, including URLs and different accounts credentials, to the contractor in charge of the penetration tests. The contractor will try to compromise and exploit the vulnerabilities found during the intrusion tests.

The contractor shall simulate attacks of the agency’s system in an attempt to gain access to sensitive data, with the purpose of determining whether a system is secure.

The contractor shall produce a Web Application Intrusion Test Report that includes an executive summary, methodology and goals, scenario and scope, attack narrative, observations and recommendations, and a conclusion.

###

#### 3.5.4.2 Static Application Security Testing (SAST) in Development Phase

SAST reviews static analysis scan results in real-time and detects security vulnerabilities within the source, binary, or byte code of applications.

The contractor shall scan an application’s source code during deployment to detect security vulnerabilities.

The contractor shall provide a Static Application Security Testing\ Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

**3.5.4.3 Dynamic Application Security Testing (DAST) in Deployment Phase**

DAST simulates controlled attacks on a running application or service to identify exploitable vulnerabilities in a running environment with no access to the application source code architecture.

The contractor shall conduct tests to find security vulnerabilities in applications while the application is running, verifying the security during run time by testing different attack types against the running application.

The contractor shall provide a Dynamic Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

#### 3.5.4.4 Interactive Application Security Testing (IAST)

IAST analyzes code for security vulnerabilities while the application is run by an automated test, human tester, or any activity “interacting” with the application’s functionality. It searches for known vulnerabilities inside the application’s functions by simulating the various scenarios in which a user runs or interacts with the application.

The contractor shall conduct tests to identify security vulnerabilities inside the application’s functions by simulating various scenarios in which a user runs or interacts with the application.

The contractor shall include an Interactive Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

####

#### 3.5.4.5 Mobile Application Security Testing (MAST) in Deployment Phase

#### MAST analyzes and identifies vulnerabilities in applications used with mobile platforms (e.g., iOS, Android, and Windows 10 Mobile) and identifies critical information exposures attributed to mobile applications in the environment.

####

#### The contractor shall analyze the security posture of new mobile technologies in development and identify critical information exposure and vulnerabilities attributed to mobile applications used with mobile platforms.

####

#### The contractor shall provide a Mobile Application Security Testing Report, including the type of vulnerability and the vulnerability location in the application’s codebase.

#### 3.5.4.6 Manual Testing in Deployment Phase

The primary goal of manual security testing is to perform secure code review to discover flaws, errors or weaknesses that lead to vulnerabilities in an application that might not be easily revealed by automated security testing alone.

The contractor shall manually test the application by executing test cases using secure code review, perform expert analysis on findings, and generate test reports without the aid of any automated AST tools.

The contractor shall provide a Test Report with an executive summary, detailed findings, and vulnerability risk analysis in the context of the application hosting environment and the agency’s mission and functions.

The contractor shall develop a Remediation Plan for found vulnerabilities. The plan will consist of the following:

* Detailed list of vulnerability findings
* Vulnerability findings prioritized by risk level
* Implementation Plan for fix / patches of vulnerabilities
* Plan for monitoring reliability of fixes

The agency will remediate vulnerabilities according to the Remediation Plan and the contractor shall validate remediated vulnerabilities by re-testing.

###

**3.5.4.7 Remediation Validation in Deployment Phase**

No sooner than <insert number of business days> business days and no later than <insert number of business days> business days of the acceptance of any test report, the contractor shall validate that any vulnerabilities identified in the test report during the deployment phase have been remediated by the agency.

The contractor shall provide a remediation validation report that lists any previously-identified vulnerabilities and whether or not they have been remediated.

### 3.5.5 Red Team Application Security Exercises

The contractor shall conduct Red Team assessments that utilize tactics used by real-life adversaries, including but not limited to, spear phishing, whaling, malicious code execution, data exfiltration, credential theft, and account abuse. The contractor will identify gaps or flaws in the defensive strategies of the organization.

Deliverables for Red Team Application Security Exercises include, but are not limited to:

* Rules of Engagement document containing the objectives, explicit restrictions, authorized target spaces and activities for the exercises. This document must be approved/signed by <insert exercise authority title> before red team exercises commence.
* Red Team Report that includes an executive summary, methodology and goals, scenario and scope, attack narrative, observations and recommendations, and a conclusion.
	+ - The contractor shall keep all information pertaining to the applications being tested and other information provided and / or captured during each assessment encrypted manner with no public access.
		- All data will be kept for a period of time agreed upon between <Insert agency name> and the contractor, after which the data shall be destroyed in a secure manner in accordance with policy and standards for destruction of digital data.

**(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 2021 / 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 revise 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 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 |
| Status Reports | Insert related SOW reference | NLT the 15th of each month |
| Test Plan Strategy  | 3.5.1.1  | NLT <insert number of days> business days after award |
| Security Impact Analysis | 3.5.1.2 | NLT <insert number of days> business days after task assignment |
| Updated Application Threat Modeling SOP | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Updated Application Threat Modeling Implementation Plan | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Updated Security Threat Response Plan | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Create and / or update the Application Threat Modeling Implementation Plan | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Create and/or update the Security Threat Response Plan | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Software Bill of Materials (SBOM) | 3.5.2.2 | NLT <insert number of days> business days after task assignment |
| Remediation Validation Report | 3.5.2.3 / 3.5.3.7 / 3.5.4.7 | NLT <insert number of days> business days after task assignment |
| Penetration Testing Rules of Engagement Document | 3.5.3.1 / 3.5.4.1 | NLT <insert number of days> business days after award |
| Penetration Test Report | 3.5.3.1 | NLT <insert number of days> business days after task assignment |
| Web Application Intrusion Testing Rules of Engagement Document | 3.5.3.1.1 | NLT <insert number of days> business days after award |
| Web Application Intrusion Test Results | 3.5.3.1.1 / 3.5.4.1.1 | NLT <insert number of days> business days after task assignment |
| Web Application Assessment Report | 3.5.3.2 | NLT <insert number of days> business days after task assignment |
| Mobile Application Security Testing (MAST) Report | 3.5.3.3 / 3.5.4.5 | NLT <insert number of days> business days after task assignment |
| Static Application Security Testing (SAST) Report | 3.5.2.1 / 3.5.3.4 / 3.5.4.2 | NLT <insert number of days> business days after task assignment |
| Dynamic Application Security Testing (DAST) Report | 3.5.3.5 / 3.5.4.3 | NLT <insert number of days> business days after task assignment |
| Test Report | 3.5.3.6 / 3.5.4.6 | NLT <insert number of days> business days after task assignment |
| Remediation Plan | 3.5.3.6 / 3.5.4.6 | NLT <insert number of days> business days after task assignment |
| Interactive Application Security Testing (IAST) Report | 3.5.4.4 | NLT <insert number of days> business days after task assignment |
| Red Team Rules of Engagement Document | 3.5.5 | NLT <insert number of days> business days after award |
| Red Team Report | 3.5.5 | NLT <insert number of days> business days after task assignment |
| <Add other deliverables as applicable> | Insert related SOW reference | NLT <insert number of days> business days after task assignment |
| Final Reports | Insert related SOW reference | 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.