**READ FIRST**

The HACS SOW templates (found on the HACS website) 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 SOC 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

Cybersecurity is the ability to protect or defend information systems from cyber-attacks. Cybersecurity is an umbrella term that incorporates different information technology (IT) strategies that protect networks (e.g., identity management, risk management, and incident management). Information Assurance employs measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating identification, protection, detection, response, and recovery capabilities. As IT evolves, so do the threats to data security, individual privacy, and the continued operation of the Federal Government’s IT assets.

<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 the following subcategories under SIN 54151HACS.

* High Value Asset (HVA) Assessment
* Risk and Vulnerability Assessment (RVA)
* Penetration Testing
* Cyber Hunt
* Incident Response

The contract shall be for non-personal services to provide SOC 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 contractor shall assist <Insert agency acronym> in the management, maintenance, and maturing of the current SOC <insert frequency, e.g. (24 hours a day, 7 days a week (24x7), 365 days a year (24x7x365)> to protect the <Insert agency acronym> information systems infrastructure. The contractor shall support traditional SOC activities and be able to support these activities during periods of Continuity of Operations (COOP) and exercises. That is, if it becomes necessary to temporarily relocate to a selected alternate site for emergency or test scenarios, the contractor must be able to support and extend normal SOC operations to that remote location. This scope of work will be accomplished through the placement of task orders.

Specific categories of tasks that fall within this scope of work, and the necessary contractor capabilities, are outlined in the following sections.

**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 (2014)* |
| **FIPS 199** | *Federal Information Processing Standards Publication (FIPS) 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 800-86** | *Guide to Integrating Forensic Techniques into Incident Response* |
| **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 800-153** | *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* |
| **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, July 2016* |
| **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 SOC 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 HACS services:

* Program Management and Control
* SOC Operations Services
* SOC Architecture, Engineering, Operations, and Maintenance
* Surge / Emerging Threat Support

# 3.5.1 PROGRAM MANAGEMENT AND CONTROL

The contractor shall perform the Program Management activities defined in this SOW, to include preparation of Task Order Management Plans, cost analyses, activity and project tracking schedules, risk registers, and risk and issue mitigation strategies for all <Insert agency acronym> SOC activities. This task consists of the following subtasks:

# Subtask 1 - Program Management

# Subtask 2 - Transition Planning

* Subtask 3 - SOC Performance and Investment Metrics
* Subtask 4 - Cybersecurity Communications / Coordination

# 3.5.1.1 Subtask 1 - Program Management

The contractor shall provide program management oversight across the contract and all contract task orders, up to and including contractual deliverables and financial controls. Deliverables for Program Management include, but are not limited to, a SOC Support Services Program Management Plan to be provided to the Director of the SOC, the Contracting Officer (CO), and the Contracting Officer's Representative (COR) within <insert number of days> calendar days of the contract award.

# 3.5.1.2 Subtask 2 - Transition Planning <if applicable>

The contractor shall support <Insert agency acronym> Government leads with transition planning and transition plan execution for the transition of SOC support services from the incumbent contractor to the successor contractor. Deliverables for Transition Planning include, but are not limited to, a contract level transition support report detailing the status of the Contract Level Transition Support requirements.

# 3.5.1.3 Subtask 3 - SOC Performance and Investment Metrics

The contractor shall coordinate with the Government <Insert agency acronym> SOC Manager and the <Insert agency acronym> SOC Chief, the <Insert agency acronym> Security Architect, and the <Insert agency acronym> Office of the Chief Information Officer (OCIO) to design, develop, and implement a SOC Performance and Investment Metrics Program.

The contractor shall maintain and execute the Performance and Investment Metrics Program and report SOC metrics that inform Chief Information Security Officer (CISO) executives and the Government SOC management team and technical staff on the overall performance of the SOC in the current reporting period, in the task order period of performance, and over the life of the contract. The contractor shall analyze and summarize (1) the impact of each significant incident and the recovery costs, (2) the capability effectiveness of Computer Network Defense (CND) sensor coverage and the operations and maintenance costs, (3) the effectiveness of the contractor’s implementation of the <Insert agency acronym> intrusion defense chain methodology, and (4) the number and categories of threats of concern identified by the SOC and supplied to the SOC by external Government agencies. Deliverables for SOC Performance and Investment Metrics include, but are not limited to, bi-weekly SOC Performance and Investment Metrics Program Summary briefings, and quarterly written reports.

# 3.5.1.4 Subtask 4 - Cybersecurity Communications /

# Coordination

The <Insert agency acronym> SOC works closely with organizations to coordinate security operations and deliver or request assistance, or assist with investigations. Security Event Notifications (SENs) are usually the products of <Insert agency acronym> SOC security event analyses, but may be generated based on information from other trusted sources. The <Insert agency acronym> SOC maintains a two-way information exchange with the U.S. Computer Emergency Readiness Team (US-CERT) and passes reports of confirmed or suspected incidents to them. The contractor shall prepare US-CERT Incident Reports, US-CERT After-Action Reports, and SOC Incident Response CONOPS for US-CERT and forward them after approval from the Government <Insert agency acronym> SOC Manager. The contractor shall comply with cybersecurity incident reporting formats and timelines as mandated by US-CERT. The contractor shall work with the <Insert agency acronym> SOC Manager to coordinate with intelligence community organizations as required. The contractor shall work with the <Insert agency acronym> SOC Manager to coordinate with law enforcement organizations as required. Deliverables for Cybersecurity Communications / Coordination include, but are not limited to, incremental updates while responding to an incident and an After Action Report, including lessons learned after an incident.

# 3.5.2 SOC OPERATIONS SERVICES

SOC Operations Services is responsible for providing support to conduct the daily business of the SOC, which includes threat monitoring and analysis, incident response, vulnerability management, along with various other activities. This task consists of the following subtasks:

* Subtask 1 - Monitoring and Analysis Support
* Subtask 2 - Digital Media Analysis (DMA) Support
* Subtask 3 - Cyber Intelligence Support
* Subtask 4 - Vulnerability Assessment Support
* Subtask 5 - Penetration Testing Support
* Subtask 6 - Incident Assessment and Response Support
* Subtask 7 - Insider Threat Hunting Support

**3.5.2.1 Subtask 1 - Monitoring and Analysis Support**

The contractor shall provide a Monitoring and Analysis support group to actively review all SOC data feeds, analytical systems, sensor platforms, and output from other SOC tool products. The contractor shall also provide written or oral reports of findings to the contractor’s program manager, the Government <Insert agency acronym> SOC Manager, and COR-designated Government SOC Operations Leads for further investigation or for action. The Monitoring and Analysis support group shall participate in a variety of Information System Security (ISS) activities, including: monitoring of systems status; escalating and reporting potential incidents; creating and updating incident cases and tickets; risk assessment analysis for High Assurance Gateway (HAG) access and Web Access Requests (WARs); analyzing ISS reports; applying various antivirus, intrusion detection, DMA, and vulnerability assessment tools, techniques and procedures; authoring and implementing custom detection content; tuning the Security Information and Event Management (SIEM) and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) events to minimize false positives; authoring and maintaining custom SIEM content; program analysis and review; hardware and software evaluation and analysis; process improvement; data management; and coordination and reporting of ISS-related incidents. The Monitoring and Analysis support group shall provide <insert schedule, e.g. 24x7x365> monitoring and analysis of all <Insert agency acronym> security feeds, including General Services Administration's (GSA) Managed Trusted Internet Protocol Services (MTIPS), Trusted Internet Connections (TIC), and Policy Enforcement Points (PEP). The contractor shall investigate and positively identify anomalous events that are detected by security devices or reported to the SOC from external entities, <Insert agency acronym> components, system administrators, and the user community, via security monitoring platform and tools, incoming phone calls, and emails.

The Monitoring and Analysis support group may also be required to participate in assembling, evaluating, installing, and maintaining various intrusion detection sensors and associated software applications. The Monitoring and Analysis support group shall provide informal investigation, review, and recommendation documentation as necessary. Deliverables for Monitoring and Analysis Support include, but are not limited to, daily summary informal reports based on security event analysis and Technical Evaluation Reports (TER).

**3.5.2.2 Subtask 2 - Digital Media Analysis (DMA) Support**

The contractor’s DMA Analysts shall perform forensic analysis on a variety of digital media devices and mediums to identify, reverse engineer, and deobfuscate content related to an incident, such as malicious content. The contractor shall, after the analyses have been performed, provide a detailed written technical Report of Findings that includes the methodology used during the DMA evaluation, the findings from the evaluations, and any recommendation for further action shall be prepared and sent to the Government DMA Lead for further evaluation and coordination. Deliverables for DMA Support include, but are not limited to, a DMA Report of Findings.

**3.5.2.3 Subtask 3 - Cyber Intelligence Support**

The contractor’s Cyber Intelligence Analysts shall provide technical expertise in cyber adversary capabilities and an assessment of the intentions of these groups to conduct Computer Network Exploitation (CNE) and Computer Network Attack (CNA) against U.S. private sector and Government networks, and information systems. Cyber Intelligence Analysts shall review the ingestion of cyber news feeds, signature updates, incident reports, threat briefs, and vulnerability alerts from external sources and determine its applicability to the <Insert agency acronym> environment. This type of information shall also be shared externally within the cyber intelligence community, such as US-CERT. Deliverables for Cyber Intelligence Support include, but are not limited to, weekly cyber intelligence reports.

**3.5.2.4 Subtask 4 - Vulnerability Assessment Support**

The contractor’s Vulnerability Assessment Analysts shall provide onsite and remote vulnerability assessment capabilities as a sustained, full-time program independent of incident detection, recovery, or reporting activities. Activities shall include full-knowledge, open-security assessment of a <Insert agency acronym> site, enclave, or system. The contractor shall work with system owners and system administrators, to holistically examine the security architecture and vulnerabilities of their systems, through security scans, examination of system configuration, review of system design documentation, and interviews. The contractor shall use network and vulnerability scanning tools, as well as invasive technologies used to interrogate systems for configuration and status. Deliverables for Vulnerability Assessment Support include, but are not limited to, a Vulnerability Assessment Report of Findings, along with recommended remediation.

**3.5.2.5 Subtask 5 - Penetration Testing Support**

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, system, and/or network. Deliverables for Penetration Testing include, but are not limited to, a Rules of Engagement document containing the type and scope of testing, and client contact details; and a Penetration Test Report that includes an executive summary, a contextualized walkthrough of technical risks, potential impact of vulnerabilities found, and vulnerability remediation options. Deliverables for Penetration Testing Support include, but are not limited to, a Penetration Testing Report of Findings.

**3.5.2.6 Subtask 6 - Incident Assessment and Response**

**Support**

The contractor shall work with the <Insert agency acronym> <Insert name and acronym of agency computer incident response unit>, and/or any other pertinent parties (to include external vendors) at any <Insert agency acronym> location to recover from any incident. In this role, the contractor shall have hands-on involvement in gathering artifacts or recovering systems. It is expected that any incident requiring a response team to be deployed shall be able to deploy within <insert number of hours> hours of notification. On rare instances where it is not possible to deploy, support will usually be done via phone and email, or, in rarer cases, remote system access. In all cases, this work shall be done in coordination with external service providers, <Insert agency acronym> system owners, system administrators, and Information System Security Officers (ISSOs), as appropriate. The contractor shall also maintain a set of Government furnished portable vulnerability assessment, digital media analysis, and malware analysis tools to support deployment missions, to be used for critical incident response efforts and in response to high priority initiatives determined by <Insert agency acronym> leadership. Deliverables for Incident Assessment and Response Support include, but are not limited to, an Incident Assessment and Response Report.

**3.5.2.7 Subtask 7 - Insider Threat Hunting Support**

The contractor shall provide support to detect, prevent, and respond to threats posed by malicious, negligent or compromised insiders, by maintaining in-depth visibility into the <Insert agency acronym> Enterprise and having a means of filtering and prioritizing threat data into concise, actionable intelligence. The contractor shall provide advanced analysis and adversary hunting support to operations in an effort to proactively uncover evidence of adversary presence on <Insert agency acronym> networks. Deliverables for Insider Threat Hunting Support include, but are not limited to, Daily Summary Reports based on security event analysis.

# 3.5.3 SOC ARCHITECTURE, ENGINEERING, OPERATIONS, AND

# MAINTENANCE

This task consists of the following subtasks:

* Subtask 1 - SOC Tool Engineering
* Subtask 2 - SOC Architecture and Strategy
* Subtask 3 - Tool Maintenance
* Subtask 4 - SOC Change and Release Management
* Subtask 5 - SOC Platform / Infrastructure Operations
* Subtask 6 - Support for COOP

**3.5.3.1 Subtask 1 - SOC Tool Engineering**

The contractor shall provide security engineering and subject matter expertise to conduct market research, product evaluation, prototyping, integration, development, deployment, recapitalization, operations, and maintenance support for a variety of SOC technologies, such as those that fall outside the scope of the GSA MTIPS contract. The contractor shall provide support for Government Furnished vulnerability assessment tools, penetration testing tools, malware analysis and digital media analysis tools, <Insert agency acronym> online incident ticketing and case tracking, host IDS/IPS, network IDS/IPS, full network traffic collection and retention, analyst workstations, SOC routers, SOC switches, SOC firewalls, SOC storage devices, SOC backup system, logging system, and the SIEM. Deliverables for SOC Tool Engineering include, but are not limited to, SOC Tool Engineering Design Documentation and Test Plans for new and existing security applications and hardware.

**3.5.3.2 Subtask 2 - SOC Architecture and Strategy**

The contractor shall advise and assist the <insert title of official in charge of security architecture> with SOC architecture activities, for all <Insert agency acronym> SOC information systems initiatives supporting all SOC tools and capabilities. Contractor advice and assistance shall be in accordance with Federal requirements, <Insert agency acronym> information system security policy, and industry best practices. The contractor shall collaborate with the OCIO to configure, build, provide recommendations, and ensure all hardware and software is IPv6 compliant with the direction set forth by the <Insert agency acronym> OCIO. Deliverables for SOC Architecture and Strategy include, but are not limited to, documentation for new or revised SOC information technology solutions.

**3.5.3.3 Subtask 3 - Tool Maintenance**

The contractor shall create procedures and documentation for maintaining all SOC hardware and software. The contractor shall perform full-scope administration, management, and configuration, patching, upgrades and optimization of SOC tools, devices and application systems, and servers and sensors. Specifically, the contractor shall provide security device signature maintenance and performance reports; maintain the SIEM to collect and aggregate IDS/IPS data from network sensors, raw data from collection agents, firewalls, proxy servers, antivirus, vulnerability scanner elements and other security-relevant devices; enroll <Insert agency acronym> Enterprise and systems information into the SIEM tool and perform asset categorization and prioritization; and install or modify network security elements, tools, and other systems as required to maintain optimal coverage and performance, as approved by the Government <Insert agency acronym> SOC Manager. Deliverables for Tool Maintenance include, but are not limited to, Market Research Reports for new hardware and software, Test Plans for the implementation of new security applications and hardware, and standard Tool Maintenance Design Documentation for new and existing security applications.

**3.5.3.4 Subtask 4 - SOC Change and Release Management**

SOC Change and Release Management is responsible for controlling and managing the life cycle of all SOC changes, with minimum disruption to SOC services. Change and Release Management oversees and manages all introductions into the production and test environments. The contractor shall provide support for Change Requests (CR) and security reviews. This requires a Subject Matter Expert (SME) to review <Insert agency acronym and name of net system> and <Insert agency acronym> engineering CRs and configuration changes, and provide recommendations as the security subject matter expert on the <Insert agency acronym> Change Control Board (CCB) and <Insert agency acronym> Interim Change Control Board (ICCB). The contractor shall provide recommendations for configuration management, and check for compliance with <Insert agency acronym> policy, standards, and hardening guidelines. The contractor shall create supporting documentation for CRs, track and manage SOC security devices, physical property, and perform asset management. The contractor shall also assist a Government Local Property Officer with documenting and maintaining inventory of SOC property and assets, documenting SOC software licenses, and tracking maintenance and support agreements. Deliverables for SOC Change and Release Management include, but are not limited to, Change and Release Design Documentation, including "end-to-end" configuration flow diagram describing all solution elements and asset locations and Test Plans.

**3.5.3.5 Subtask 5 - SOC Platform / Infrastructure Operations**

SOC Platform / Infrastructure Operations is responsible for ensuring that the SOC platform itself is available and operational. This includes the shared application and technical services, as well as the system software, middleware, information security infrastructure, networks and data centers. Deliverables for SOC Platform / Infrastructure Operations will be provided in individual task orders.

**3.5.3.6 Subtask 6 - Support for COOP**

At the contract-level, the contractor shall provide support personnel to the COOP site to support daily operations when the <Insert agency acronym> SOC COOP Status is invoked by the Government <Insert agency acronym> SOC Manager. COOP Status for the <Insert agency acronym> SOC, as defined in National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), and the National Continuity Policy Implementation Plan (NCPIP), is intended to ensure that <Insert agency acronym> SOC Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. <Insert agency acronym> SOC PMEFs are defined in the <Insert agency acronym> SOC COOP Plan. The contractor shall participate in <Insert agency acronym> SOC COOP Status exercises and tests.

The contractor shall provide services supporting <Insert agency acronym> SOC PMEFs at the COOP SOC site within 48 hours after the <Insert agency acronym> SOC COOP Status is invoked by the Government <Insert agency acronym> SOC Manager. As defined in the <Insert agency acronym> SOC COOP Plan, the contractor shall ensure that all SOC cybersecurity feeds are directed to or accessible from the COOP SOC site and activate operation of electronic bonding with the COOP SOC site to enable contractor and Government performance of all <Insert agency acronym> SOC PMEFs. The contractor shall ensure that all, or a COR approved subset, of the contractor’s <Insert agency acronym> SOC staff are onsite at and prepared to work the COOP, as scheduled, until the <Insert agency acronym> SOC COOP Status is canceled by the COR. Deliverables for Support for COOP include, but are not limited to, a COOP Plan.

# 3.5.4 SURGE / EMERGING THREAT SUPPORT

The contractor shall support tasks in Section 3 with Surge Support or in response to an Emerging Threat upon notification by the Government and via the issuance of a task order or the funding of a surge Contract Line Item Number (CLIN). Deliverables for Surge / Emerging Threat Support will be provided in individual task orders.

#

**(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 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 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** |
| --- | --- | --- |
| 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 |
| SOC Support Services Program Management Plan  | 3.5.1.1 | NLT 15 calendar days after award |
| Transition Support Report  | 3.5.1.2 | NLT <insert number of days> business days after award |
| Bi-weekly SOC Performance and Investment Metrics Program Summary Briefings | 3.5.1.3  | Bi-weekly intervals starting <insert number of days> business days after award |
| Quarterly Written Performance Reports | 3.5.1.3 | Quarterly intervals starting <insert number of days> business days after award |
| Incident After Action Report  | 3.5.1.4  | NLT <insert number of days> business days after task assignment |
| Technical Evaluation Reports  | 3.5.2.1 | NLT <insert number of days> business days after task assignment |
| Daily Summary Informal Reports  | 3.5.2.1 | Daily intervals starting <insert number of days> business days after award |
| DMA Report of Findings  | 3.5.2.2  | NLT <insert number of days> business days after task assignment |
| Weekly Cyber Intelligence Reports  | 3.5.2.3 | Weekly intervals starting <insert number of days> business days after award |
| Vulnerability Assessment Report of Findings  | 3.5.2.4 | NLT <insert number of days> business days after task assignment |
| Penetration Testing Report of Findings  | 3.5.2.5 | NLT <insert number of days> business days after task assignment |
| Incident Assessment and Response Report  | 3.5.2.6 | NLT<insert number of days> business days after task assignment |
| Daily Summary Reports based on Security Event Analysis  | 3.5.2.7 | Daily intervals starting <insert number of days> business days after task assignment |
| SOC Tool Engineering Design Documentation  | 3.5.3.1 | NLT <insert number of days> business days after task assignment |
| Test Plans for New and Existing Security Applications and Hardware | 3.5.3.1 | NLT <insert number of days> business days after task assignment |
| Documentation for New or Revised SOC Information Technology Solutions  | 3.5.3.2 | NLT <insert number of days> business days after task assignment |
| Test Plans for Implementation of New Security Applications and Hardware | 3.5.3.3 | NLT <insert number of days> business days after task assignment |
| Tool Maintenance Design Documentation for New and Existing Security Applications | 3.5.3.3 | NLT <insert number of days> business days after task assignment |
| Market Research Reports for New Hardware and Software | 3.5.3.3 | NLT <insert number of days> business days after task assignment |
| Change and Release Design Documentation  | 3.5.3.4 | NLT <insert number of days> business days after task assignment |
| COOP Plan  | 3.5.3.6 | 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.