**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 Cyber Hunt 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 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 holding the Multiple Award Schedule Information Technology (MAS IT) HACS SIN. Additionally, the contractor must be cataloged in the following subcategory under SIN 54151HACS.

* Cyber Hunt

The contract shall be for nonpersonal services to provide HACS 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 Cyber Hunt 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 amended:

| **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 activities for Cyber Hunt services. 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)]

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

# 3.5.1 Cyber Hunt

The primary purpose of Cyber Hunt services is to proactively and iteratively detect, isolate, and neutralize advanced threats that evade automated security solutions. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Cyber Hunt activities use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks, and investigate and analyze all relevant response activities.

Cyber Hunt tasks include: collecting intrusion artifacts (e.g., source code, malware, and trojans) and using discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; coordinating with and providing expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; and correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. Deliverables for Cyber Hunt include, but are not limited to, a Cyber Hunt Report including an artifact list, a summary of potential incidents and resolved incidents, and remediation recommendations for vulnerabilities found based on previous incident data.

Knowledge Areas include, but are not limited to:

* Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])
* Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)
* Knowledge of incident categories, incident responses, and timelines for responses
* Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
* Develops cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.
* Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
* Conducts advanced analysis of collection and open-source data to ensure target continuity, profile targets and their activities, and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.
* Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

**(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 |
| Status Reports | Insert related SOW reference | NLT the 15th of each month |
| Rules of Engagement | Insert related SOW reference | NLT <insert number of days> business days after award |
| Cyber Hunt Report | 3.5.1 | 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 |

## 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.