**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 HVA Assessment 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.

* High Value Asset (HVA) Assessment

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 HVA assessment 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 an HVA Assessment. 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 HVA Assessment HACS services:

* Risk and Vulnerability Assessment
* Security Architecture Review
* System Security Engineering

# 3.5.1 Risk and Vulnerability Assessment (RVA)

RVAs conduct assessments of threats and vulnerabilities; determine deviations from acceptable configurations, enterprise, or local policy; assess the level of risk; and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations. Tasks include, but are not limited to:

* Penetration Testing
* Network Mapping
* Vulnerability Scanning
* Phishing Assessment
* Wireless Assessment
* Web Application Assessment
* Operating System Security Assessment (OSSA)
* Database Assessment

# 3.5.1.1 Subtask 1 - Penetration Testing

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, 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.

Knowledge and skills required for Penetration Testing include, but are not limited to:

* Knowledge of system and application security threats and vulnerabilities
* Skill in the use of social engineering techniques
* Skill in using penetration testing tools
* Knowledge of general attack stages

# 3.5.1.2 Subtask 2 - Network Mapping

The contractor shall identify assets on an agreed upon IP address space or network range(s). Deliverables for Network Mapping include but are not limited to a network map of the organization’s system that includes a visual representation of the organization's physical devices and digital network.

Knowledge and skills required for Network Mapping include but are not limited to:

* Knowledge of network security architecture concepts including topology, protocols, components, and principles
* Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration Protocol (DHCP), domain name system, and directory services
* Ability to generate and implement capabilities to monitor organization’s network in real-time

 **3.5.1.3 Subtask 3 - Vulnerability Scanning**

The contractor shall comprehensively identify IT vulnerabilities associated with agency systems that are potentially exploitable by attackers. Deliverables for vulnerability scanning include but are not limited to a Vulnerability Scanning Risk Assessment that includes an executive summary and risk assessment reports and/or dashboards.

Knowledge and skills required for Vulnerability Scanning include but are not limited to:

* Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems
* Skill in using network analysis tools to identify vulnerabilities
* Ability to identify systemic security issues based on the analysis of vulnerability and configuration data

 **3.5.1.4 Subtask 4 - Phishing Assessment**

The contractor shall complete activities to evaluate the level of awareness of the agency workforce with regard to digital form of social engineering that uses authentic looking, but falsified, emails requesting information from users or direct them to a fake website that requests information. Phishing assessments can be conducted as a one-time event or as part of a larger campaign to be conducted over several months. Deliverables for a Phishing Assessment include, but are not limited to, a Phishing Assessment Report that includes an executive summary and metrics that highlight potential weaknesses in an organization's email policy.

Knowledge and skills required for a Phishing Assessment include but are not limited to:

* Skill in the use of digital social engineering techniques

**3.5.1.5 Subtask 5 - Wireless Assessment**

The contractor shall include wireless access point detection, penetration testing, or both. A wireless assessment is performed while onsite at a customer’s facility. Deliverables for a Wireless Assessment include but are not limited to a Wireless Assessment Report that includes an executive summary, networking mapping, vulnerability analysis, and a wireless network configuration assessment on the wireless system.

Knowledge and skills required for a Wireless Assessment include but are not limited to:

* Knowledge of wireless security threats and vulnerabilities
* Skill in the use of social engineering techniques
* Knowledge of general attack stages

**3.5.1.6 Subtask 6 - Web Application Assessment**

The contractor shall provide 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. Deliverables for Web Application Assessment include but are not limited to 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.

Knowledge and skills required for a Web Application Assessment include but are not limited to:

* Knowledge of system and application security threats and vulnerabilities
* Skill in the use of social engineering techniques
* Knowledge of general attack stages

**3.5.1.7 Subtask 7 - Operating System Security Assessment**

**(OSSA)**

The contractor shall assess the configuration of select host operating systems against standardized configuration baselines. Deliverables for OSSA include but are not limited to an OSSA Report that includes an executive summary and a vulnerability analysis.

Knowledge and skills required for OSSA include but are not limited to:

* Knowledge of organizational baselines and configuration management systems
* Knowledge of security content automation protocols (SCAP) and operating system hardening guidelines
* Ability to identify systemic security issues based on the analysis of vulnerability and configuration data

 **3.5.1.8 Subtask 8 - Database Assessment**

The contractor shall assess the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities. Deliverables for Database Assessment include but are not limited to a Database Assessment Report that includes an executive summary, privacy assessment, and vulnerability assessment.

Knowledge and skills required for a Database Assessment include but are not limited to:

* 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 database security threats and vulnerabilities
* Knowledge of relational database management systems (RDBMS)

# 3.5.2 Security Architecture Review (SAR)

SAR evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. Architecture strengths and findings are documented in a SAR Report.

Knowledge and skills required for a SAR include but are not limited to:

* Ability to perform architecture design reviews
* Ability to perform system configuration and log reviews
* Ability to perform network traffic analyses

#

# 3.5.3 System Security Engineering (SSE)

SSE identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle.

The contractor shall provide system engineering and architectural design support

services. All strategic engineering activities will be defined and scheduled by <Insert organization name>. These <Insert organization name> directed services include:

* Studies and analysis of proposed operations modifications
* Identification and documentation of alternative operations solutions
* End-to-end architecture tradeoff assessment
* Development of strategic and tactical plans
* Implementation plans and strategies
* Standards development
* Evaluation of new program requirements
* Investigation and development of new technologies for possible operations modifications

**(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 | 3.5.1.1 | NLT <insert number of days> business days after award |
| Penetration Test Report | 3.5.1.1 | NLT <insert number of days> business days after task assignment |
| Network Map | 3.5.1.2 | NLT <insert number of days> business days after task assignment |
| Vulnerability Scanning Risk Assessment | 3.5.1.3 | NLT <insert number of days> business days after task assignment |
| Phishing Assessment Report | 3.5.1.4 | NLT <insert number of days> business days after task assignment |
| Wireless Assessment | 3.5.1.5 | NLT <insert number of days> business days after task assignment |
| Web Application Assessment Report | 3.5.1.6 | NLT <insert number of days> business days after task assignment |
| OSSA Report | 3.5.1.7 | NLT <insert number of days> business days after task assignment |
| Database Assessment | 3.5.1.8 | NLT <insert number of days> business days after task assignment |
| SAR Report | 3.5.2 | 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.