Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) 54151HACS Ordering Procedure

Overview

In collaboration with the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Management and Budget (OMB), GSA developed HACS SIN to make it easier for agencies to procure quality cybersecurity services. The HACS SIN is part of the Multiple Award Schedule (MAS) Information Technology and is designed to provide government organizations with access to qualified cybersecurity vendors and to help organizations meet IT security requirements outlined in:

- OMB Memorandum 19-03, "Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program"
- OMB Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"
- The CISO Handbook, published on https://cio.gov

The scope of the HACS SIN includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services to identify and protect a customer's information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge. It encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

- The seven-step RMF includes preparation; information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA), which evaluates organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization's incident management functions.
- SOC services are services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

There are six subgroups under the HACS SIN. Vendors listed within each subgroup in GSA eLibrary have passed a technical evaluation for that specific subgroup:

1. High Value Asset Assessments
2. Risk and Vulnerability Assessment
3. Cyber Hunt
4. Incident Response

5. Penetration Testing
6. Incident Handling and Event Management

Customer agencies should check the subgroups aligned with the services they need to ensure the vendors they select are listed under the appropriate subgroup.
The HACS SIN enables GSA to provide federal, state, local, territorial, and tribal government entities with quick, reliable access to pre-vetted vendors poised to offer key proactive, reactive, and remediation services before, during, and after the realization of cyber threats.

Table 1: Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN)

Subgroup	Description
High Value Asset (HVA) Assessment	HVA Assessments include ***Risk and Vulnerability Assessment (RVA)*** which assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA subgroup include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. ***Security Architecture Review (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. The SAR uses the RMF when designing and implementing the seven tenets of zero trust architecture by describing how the steps in the RMF map to similar steps described in NIST Special Publication (SP) 800-207, Zero Trust Architecture. ***Systems Security Engineering (SSE)*** identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to, the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.
Risk and Vulnerability Assessment (RVA)	RVA assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.
Cyber Hunt	Cyber Hunt activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

Subgroup	Description
Incident Response	Incident Response services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.
Penetration Testing	Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.
Incident Handling and Event Management	IHEM ensures that appropriate response activities are conducted when incidents and events are detected. These activities are meant to prevent or reduce impact to enterprise operations and/or security in accordance with multiple industry sources, including National Institute of Standards and Technology (NIST). Functionality includes monitoring organizational assets for deviations from expected activity; detecting and declaring incidents and events; performing analysis, triage, and containment when necessary; and performing remediation and recovery steps**.**

Benefits to Federal Agencies

- The HACS SIN is available through MAS Information Technology and is a well-managed Tier 2 Spend Under Management (SUM) vehicle, the use of which aligns with OMB Memorandum 19-13 “Category Management: Making Smarter Use of Common Contract Solutions and Practices.”

- This SIN allows agencies to easily identify high-quality cybersecurity vendors within various socioeconomic categories.

- The SIN also enables rapid ordering and deployment of services using MAS Information Technology streamlined ordering procedures that reduce procurement lead times.

- Helpful acquisition documents, such as Request for Quote (RFQ) and Statements of Work (SOWs) templates and samples are available on the Acquisition Gateway and the GSA cybersecurity website http://www.gsa.gov/hacs.

- The HACS Independent Government Cost Estimate (IGCE) Calculation Tool is based off of pricing from HACS Vendors. It is available on the IT Security Hallway on the Acquisition Gateway.

- Cybersecurity and acquisition subject matter experts (SME) are available to help with HACS procurements. Request SME support by sending an email to ITSecurityCM@gsa.gov.

Ordering Process for the HACS SIN on MAS Information Technology

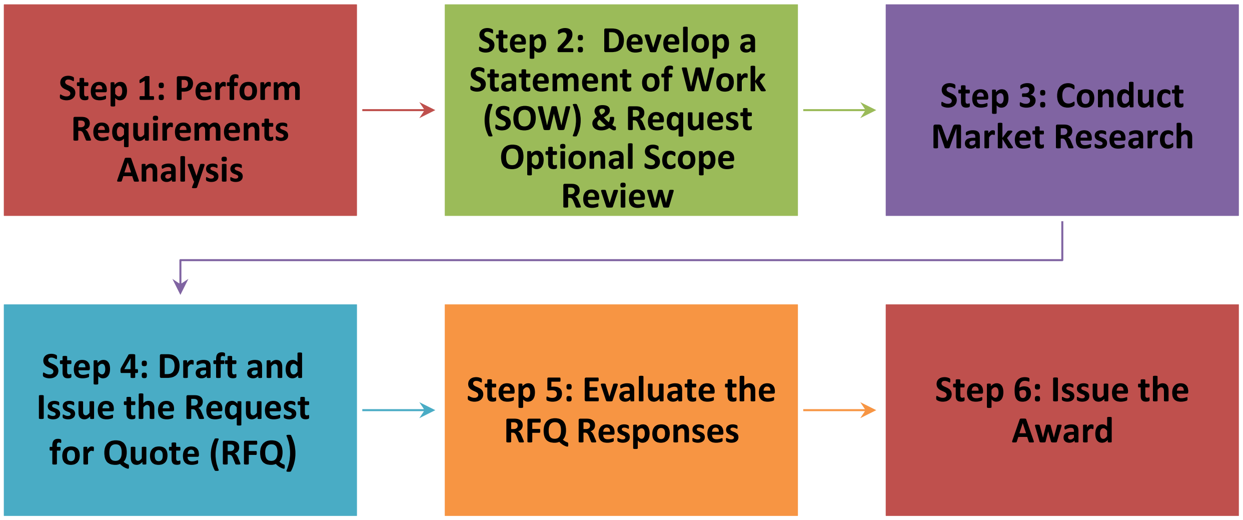
Purchases can be made through GSA Advantage!® eBuy system, by issuing a Request for Quote (RFQ) against the HACS SIN and allowing HACS vendors to respond to your requirements. An RFQ may be posted to GSA’s eBuy, an electronic RFQ system that is part of the suite of tools which complement GSA Advantage!®. The eBuy system allows ordering activities to post an RFQ, obtain quotes, and issue orders. In general, the process below should be followed to order HACS services.

When multiple requirements are needed, ordering activities should only select the HACS SIN when submitting the RFQ on eBuy, and write within the solicitation document that vendors may utilize other SINs to create a complete solution. This will ensure the responding vendors are limited to those on the HACS SIN and have passed a technical evaluation.

State and local governments may also order from the MAS Information Technology, which has cooperative purchasing (www.gsa.gov/stateandlocal.) Agencies should also comply with their organization's respective acquisition rules.

The figure and steps below provide details on the HACS ordering process.

Figure 1: HACS Ordering Process



Step 1: Perform Requirements Analysis

Step 2: Develop a Statement of Work (SOW) & Request Optional Scope Review

Step 3: Conduct Market Research

Step 4: Draft and Issue the Request for Quote (RFQ)

Step 5: Evaluate the RFQ Responses

Step 6: Issue the Award

1. Perform a requirements analysis and then follow the ordering process outlined in the Federal Acquisition Regulation (FAR) 8.405-2, Ordering Procedures for Services requiring an SOW. As described in the FAR, these procedures pertain to services priced at hourly rates as established by Schedule contracts. Vendors respond to the SOW with a quote.

2. All SOWs shall include:
   a. A description of work to be performed;
   b. Location of work;
   c. Period of performance;
   d. Deliverable schedule;
   e. Applicable performance standards; and
   f. Any special requirements (e.g., security clearances, travel, and special knowledge). To the maximum extent practicable, agency requirements shall be performance-based statements (see subpart 37.6).

3. Conduct market research using the tools below:
   a. GSA Advantage!® can help you find technology products and services. Browse the industry partners catalog and/or their price lists, which will offer details such as delivery area, environmental attributes, and warranties.
   b. GSA eLibrary can help you review an industry partner's solicitation, terms and conditions, clauses, and socioeconomic status. It can also help you find a source within a particular geographic location. GSA eLibrary is the official online resource for complete GSA Schedules contract award information.

4. Draft and issue the RFQ (contains the SOW and evaluation criteria). The RFQ shall specify the type of order (Firm Fixed Price [FFP] or Time and Materials [T&M]/Labor Hour) and include any options and any supplemental agency clauses as applicable (e.g., Defense Federal Acquisition Regulation Supplement [DFARS] for Department of Defense [DoD]).
   - **Optional:** Request a scope review through ITSecurityCM@gsa.gov.
     Follow the eBuy tutorial, which will guide you through issuing an RFI or RFQ. Posting an RFQ on eBuy is one medium for providing fair notice in accordance with FAR 8.405-2 ordering procedures for schedules.

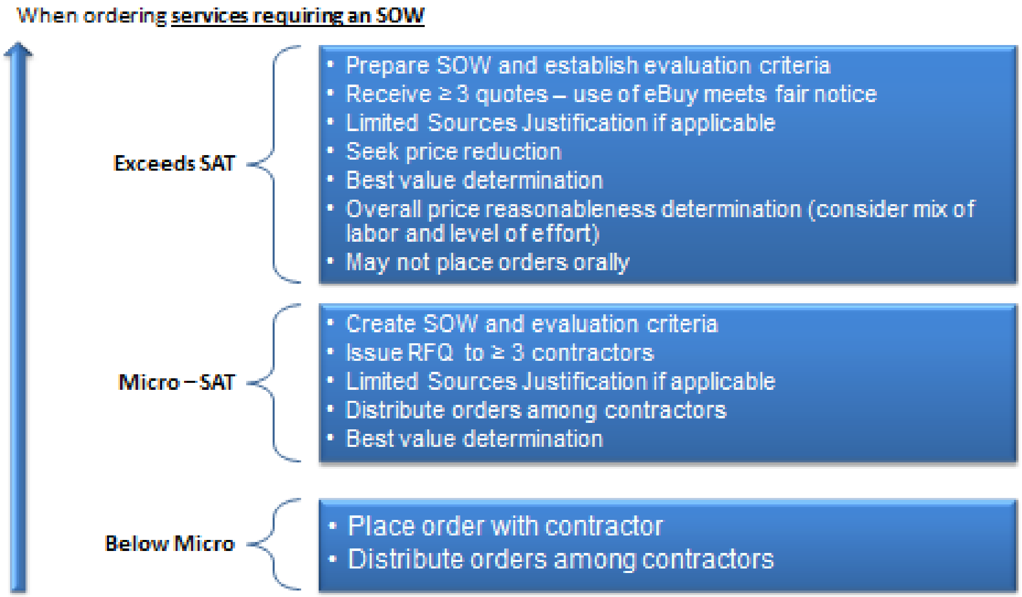
5. Evaluate the responses you receive. For an RFI, evaluate if enough vendors exist for adequate competition of the requirements on the SIN. If so, move forward with an RFQ. For an RFQ, evaluate the quote. Use GSA eLibrary to investigate the industry partners and research their detailed contract information. Use GSA eLibrary to ensure the vendor is listed under the desired HACS SIN subgroup.

6. Make the award through a paperless contracting system, such as the Standard Procurement System (SPS), ConWrite, and other eProcurement tools.

Ordering Process for HACS (FAR 8.405-2)

The figure and steps below provide details on the HACS ordering process related to the Simplified Acquisition Threshold (SAT).

Figure 2: HACS Ordering Process related to the SAT



When ordering services requiring an SOW

Exceeds SAT

- Prepare SOW and establish evaluation criteria
- Receive ≥ 3 quotes – use of eBuy meets fair notice
- Limited Sources Justification if applicable
- Seek price reduction
- Best value determination
- Overall price reasonableness determination (consider mix of labor and level of effort)
- May not place orders orally

Micro – SAT

- Create SOW and evaluation criteria
- Issue RFQ to ≥ 3 contractors
- Limited Sources Justification if applicable
- Distribute orders among contractors
- Best value determination

Below Micro

- Place order with contractor
- Distribute orders among contractors

(See also GSA MAS Desk Reference)

Support for Your HACS Procurement

- Experts are available to advise federal agencies on procurements.
- The IT Security Division also is available to conduct a scope and SME review.
- SOW and RFQ templates are available at the bottom of the HACS portal webpage.
- For more information on how to order on GSA's MAS Information Technology, please visit: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it.
- Contact the IT Security Division at ITSecurityCM@gsa.gov or please visit the HACS webpage at http://www.gsa.gov/hacs to learn more.