IT Security: GSA's Highly Adaptive Cybersecurity Services (HACS) Tool Kit

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 the MAS Information Technology HACS SIN 132-45 (legacy) / 54151HACS (new). The HACS SIN makes it easier for agencies to procure quality cybersecurity services. The SIN is designed to provide government organizations with access to 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 Chief Information Security Officer (CISO) Handbook, published on https://cio.gov

The scope of the HACS SIN includes proactive and reactive cybersecurity services. Assessment services needed for systems categorized as High Value Assets (HVA) are also within scope of this SIN. It includes Risk and Vulnerability Assessments (RVA), Security Architecture Review (SAR), and Systems Security Engineering (SSE). Additionally, the scope of the SIN includes services for the seven step Risk Management Framework (RMF), and Security Operations Center (SOC) services.

- The seven-step RMF includes preparation, information security categorization, control selection, implementation, assessment, system and common control authorizations, and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessments (ISCMA) which evaluate 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 five subcategories under the HACS SIN. Vendors listed within each subcategory in GSA eLibrary have passed a technical evaluation for that specific subcategory:

- High Value Asset Assessments - include 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. See the section below on RVA for details on those services. 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. 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 - 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 subcategory include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

- 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.

- 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 - is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

Purchases can be made through the GSA Advantage!® or 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!. eBuy 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 writing 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 MAS Information Technology, which has cooperative purchasing (www.gsa.gov/stateandlocal and https://www.gsa.gov/portal/content/202285). Agencies should also comply with their organization's respective acquisition rules.

Benefits of Using the HACS SIN

- 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 the President's Management Agenda and 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 with various socioeconomic categories.

- The SIN also enables rapid ordering and deployment of services using MAS Information Technology's streamlined ordering procedures that reduce procurement lead times by 25 to 50 percent compared to open market ordering, which is less efficient and can carry additional risks.

- Our Ordering Guide can help procurement officials rapidly solicit services from the HACS SIN.

- Helpful acquisition documents, such as Statement of Work (SOW) templates, are available on the Acquisition Gateway and GSA's IT Security website at https://gsa.gov/itsecurity.

- Cybersecurity and acquisition subject-matter experts are available to help with HACS procurements.

Statement of Work and Request for Quote Templates

The HACS SOW templates below provide example information for a variety of cybersecurity services that can be purchased through the HACS SIN. Sections 3.0 and 4.0 of each template provide typical language for a cybersecurity solicitation and provide examples of specific activities and deliverables associated with HACS.

Each template aligns with the HACS RFQ Template, and material from any of these 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.

- RFQ HACS Support Template [DOCX - 77 KB]
- SOW HACS HVA Support Template [DOCX -36KB]
- SOW HACS RMF Support Template [DOCX - 41 KB]
- SOW HACS SOC Support Template [DOCX - 40 KB]
- SOW HACS Cyber Hunt Support Template [DOCX - 62 KB]

Ordering Guide

- HACS Order Guide [DOCX - 78.1 KB]

HACS IGCE Calculation Tool

- HACS IGCE Calculation Tool [XLSX - 389KB]

HACS SIN Modernization Customer Event Presentation April 15th, 2019

- HACS SIN Modernization Customer Event Presentation

HACS SIN Slipsheet

- HACS SIN Slipsheet