Max Cybersecurity LLC Awarded Highly Adaptive Cybersecurity Services (HACS)

54151HACS (new)

The Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) is available through the Multiple Award Schedule (MAS) Information Technology. HACS provides agencies quicker access to key support services from technically evaluated vendors that will:

- Expand agencies' capacity to test their high-priority IT systems;
- Rapidly address potential vulnerabilities; and
- Stop adversaries before they impact our networks.

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, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA) which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization's incident management functions.

High Value Asset 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. See the section below on RVA for details on those services. 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. 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 – 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.

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.

Contact Us. Info@maxcybersecurity.com