This is a notice of intent to issue a modification to task order 70RSAT25FC0000007 for Information Technology Support Services (ITSS) issued against Blanket Purchase Agreement (BPA) 70RSAT22A00000001 with Silosmashers, Inc., 12001 Sunrise Valley Drive, Suite 202, Reston, VA 20191. The task order will be modified to extend performance for 10 months with a 2-month option period on a non-competitive basis. The statutory authority permitting other than full and open competition is 41 U.S.C. 3304(a)(1) implemented by the FAR Subpart 6.103-1 (FAR Class Deviation 25-11) entitled "Only One Responsible Source and No Other Supplies or Services Will Satisfy Agency Requirements."

Background

This modification to existing task order 70RSAT25FC0000007 for Information Technology Support Services (ITSS) will maintain support services to Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Office of the Chief Information Officer (OCIO) in the areas of program management, business management, enterprise architecture alignment, IT governance, and regulatory compliance for platforms such as SharePoint, ServiceNow, and Microsoft Power Platform. The task order includes labor, travel, and materials necessary to assist DHS S&T OCIO fulfill its mission. The task order has a period of performance that began on September 30, 2025, and will expire on July 31, 2026, unless extended. The market research for the re-compete of 70RSAT25FC0000007 is under development. Due to the lapse in DHS appropriations in FY26, preparations for the re-compete have been significantly delayed.

Silosmashers is the current contractor for the requirement, and they possess unique and specialized knowledge of DHS S&T CIO requirements, activities, and stakeholders to ensure seamless, continuous support during the acquisition activities required for the re-compete. Efforts to conduct a competitive procurement and then potentially transition to a new contractor prior to the end of the current period of performance would introduce unacceptable risk to ongoing S&T CIO activities and potential delays, misalignment with stakeholder and partner expectations, and significant loss of continuity in execution. Anything other than an extension of the existing task order would seriously and materially compromise the work of the S&T OCIO and the mission of DHS.

The information provided below provides an overview of the specific critical activities the current contractor will perform:

Enterprise Architecture (EA) Alignment and Maintenance
Critical Activity:

The incumbent contractor plays an essential role in guiding and supporting the development, implementation, and ongoing maintenance of a comprehensive, enterprise-wide IT strategy and architecture for S&T. This work ensures that S&T's IT portfolio remains fully aligned with federal mandates—including frameworks such as FEAF, TOGAF, and DoDAF, and that all activities comply with DHS Enterprise Architecture requirements and Technology Business Management (TBM) standards.

Risk if Performed by Another Contractor:
Without a transition period, a new contractor would lack critical context, increasing the risk of misalignment, duplication of efforts, and inefficiencies. Additionally, any lapse in continuity could result in non-compliance with federal and DHS mandates, which may lead to audit findings, funding delays, or system vulnerabilities. Finally, the disruption of ongoing strategic initiatives could delay critical modernization efforts, directly impacting mission delivery and operational effectiveness.

Information Assurance (IA) and Information System Security Officer (ISSO) Support
Critical Activity:
The current contractor's Information System Security Officers (ISSOs) serve as principal advisors on all matters related to the security of S&T's information systems. Their responsibilities include implementing DHS 4300 policy, managing day-to-day security operations, maintaining IT Security Plans, conducting vulnerability scans, responding to Information Security Vulnerability Messages (ISVMs), and supporting classified systems and Sensitive Compartmented Information Facilities (SCIFs).

Risk if Performed by Another Contractor:
The inability to transition these duties to a new contractor would pose a substantial risk to S&T's security posture. ISSO roles require continuous awareness of system configurations, vulnerabilities, and remediation actions, all of which are built on established knowledge and experience with S&T's unique environment. A new contractor would not have immediate access to this information, increasing the likelihood of security incidents or compliance failures. Furthermore, unfamiliarity with existing systems and processes could delay responses to vulnerabilities and classified system requirements, potentially exposing sensitive data. The established relationships with federal stakeholders, SCIF management, and COMSEC support are also critical to effective coordination and trust; these relationships would be disrupted, further increasing risk.

IT Operations and Maintenance (O&M) Oversight and Help Desk Support
Critical Activity:
The contractor is responsible for the daily oversight of all IT support functions, including Tier 1 and Tier 2 help desk services, network infrastructure maintenance, asset management, patch management, and after-hours emergency support. This work is essential to maintaining uninterrupted IT operations across S&T.

Risk if Performed by Another Contractor:
If another contractor were to assume these responsibilities without a proper transition period, S&T would likely experience service disruptions due to gaps in support coverage, delayed incident resolution, and a loss of continuity in asset tracking and inventory management. New personnel may not be fully trained on S&T-specific workflows, tools (such as ServiceNow), or escalation procedures, which could result in non-compliance with established service level agreements and decreased user satisfaction. Additionally, asset management and inventory processes require a high degree of accuracy and consistency; a new contractor without a transition period may introduce errors or fail to maintain proper documentation, negatively impacting audit readiness and property accountability.

If the current task order is not extended while the recompete is completed, the Agency mission would be jeopardized, and S&T CIO would lose the ability to integrate innovative technology into everyday use by the DHS operational components. DHS S&T IT support will include all hardware, networks, enterprise architecture, information assurance and service delivery support. DHS S&T requires this support to maintain and evolve its organizations required to meet mission needs.

Period of Performance: The ITSS task order requires an extension of 10 months from August 1, 2026, through May 31, 2027.

A determination by the Government to modify the existing task order without competition based upon responses to this notice is solely at the discretion of the Government.

This is a notice of the intent to modify a task order on a sole source basis. It is published for informational purposes only and not a request for competitive proposals. Therefore, no solicitation document exists for this requirement. Any firm believing that they can fulfill the requirement may be considered by the agency. Interested parties may identify their interest and capabilities in response to this synopsis. All questions and/or comments regarding this notice shall be addressed in writing to the Contracting Officer, Danette.Williams@hq.dhs.gov.