JUSTIFICATION AND APPROVAL FOR OTHER THAN FULL AND OPEN COMPETITION
41 U.S.C. 3304(a)(1)

FY26-0159

Pursuant to the requirements of the Competition in Contracting Act (CICA) as implemented by the Revolutionary Federal Acquisition Regulation Overhaul (RFO) 6.103 (Class Deviation 25-11[1]) and in accordance with the requirements of RFO 6.104, the justification for the use of the statutory authority under RFO 6.103 is justified by the following facts and rationale required under RFO 6.104-1 as follows:

1. **Agency and Contracting Activity.**

   The Department of Homeland Security (DHS), Office of Procurement Operations (OPO), Science and Technology Acquisitions Division (S&TAD), proposes to enter into a task order modification on the basis of other than full and open competition.

2. **Nature and/or Description of the Action being Approved.**

   (a) Nature of action:

   DHS intends to issue a modification to existing task order 70RSAT25FC0000007 for Information Technology Support Services (ITSS) issued against Blanket Purchase Agreement (BPA) 70RSAT22A00000001 with Silosmashers, Inc. (Silosmashers) for 10 months on a non-competitive basis. Silosmashers' has the capability and the required resources to continue to perform the in-scope services as identified below.

   (b) Name and address of the contractor:

   Silosmashers, Inc.
   12001 Sunrise Valley Drive
   Suite 202
   Reston, VA 20191

   (c) Contract type: Time and Materials (T&M)

[1] In this document, citations to RFO Parts 6, 10, 15, 25 are citations specifically to FAR Class Deviation 25-11 for FAR Part 6, FAR Class Deviation 25-06 for FAR Part 10, FAR Class Deviation 26-08 R1 for FAR Part 15, and FAR Class Deviation 25-09 R1 for FAR Part 25, which were issued as part of the Revolutionary FAR Overhaul (RFO), implemented in response to Executive Order 14275, ***Restoring Common Sense to Federal Procurement***, signed April 15, 2025.

Background information about the requirement.

This modification to existing task order 70RSAT25FC0000007 will maintain support services to DHS S&T Office of the Chieflnfonnation Office (OCIO) in the areas of program management, business management, enterprise architecture alignment, IT governance, and regulatory compliance for platfonns such as SharePoint, ServiceNow, and Microsoft Power Platfonn. 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 perfonnance that began on September 30, 2025, and will expire on July 31, 2026, unless extended. The market research report for the recompete of 70RSAT25FC0000007 is under development. Due to the lapse in DHS appropriations in FY26, preparations for the re-compete have been significantly delayed.

3. Description of Supplies/Services.

The ITSS task order provides technology, property, security, and processes for approximately 2,000 staff in Washington, D.C. and laboratories in New York, New Jersey, Maryland, Alabama and Florida. It supports 32 distinct IT Systems with currently 2,000 endpoints and projects. It provides professional technical support services to assist the organizations, missions, functions, and objectives enabling DHS S&T to integrate innovative technology into everyday use by DHS operational components. DHS S&T infonnation teclmology (IT) support includes all hardware, networks, enterprise architecture, information assurance and service delivery support. DHS S&T requires this support to maintain and evolve its organizations.

4. **Identification of Statutory Authority Permitting Other Than Full and Open Competition.**

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."

5. **Demonstration that the proposed contractor's unique qualifications or the nature of the acquisition requires use of the authority cited**:

(a) Rationale for using the authority cited in section 4 of the J&A.

The ITSS task order requires an extension of 10 months from August 1, 2026, through May 31, 2027. Silosmashers is the current contractor for the requirement, and they possess unique and specialized knowledge of DHS S&T CIO requirements, activities, and stakeholders. 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 acquisition execution. Anything other than an extension of the existing task order would seriously and materially compromise the work of S&T and the mission of DHS. See below specific critical activities the current contractor will perform, along with the risks associated if another contractor were to perform these activities:

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 Federal Enterprise Architecture Framework (FEAF), The Open Group Architecture Framework (TOGAF), and Department of Defense Architecture Framework (DoDAF), and that all activities comply with DHS Enterprise Architecture requirements and Technology Business Management (TBM) standards.

Risk if Performed by Another Contractor:
If these responsibilities were transitioned to a new contractor, S&T would face a significant loss of institutional knowledge. The current vendor has designed, implemented, and actively maintains the S&T Directorate's enterprise architecture (EA) framework, which is fully aligned with federal standards such as FEAF, TOGAF, and DoDAF, and integrates Technology Business Management (TBM) methodologies. The incumbent's EA team has authored and continuously updates S&T's authoritative architecture documentation, technical reference models (TRM), and governance policies. These artifacts are foundational to ongoing IT investments, modernization efforts, and compliance reporting. A new contractor would face a steep learning curve due to the complexity and specificity of S&T's architecture. A new vendor would need to familiarize themselves with the existing

EA artifacts, custom integrations, and ongoing modernization initiatives. 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.

Information Assurance (IA) and Information System Security Officer (ISSO) Support

Critical Activity:
The contractor's Information System Security Officers (ISSOs) serve as support to federal personnel 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:
Transitioning 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. The current contractor/vendor distinguishes itself through proprietary automation and integration solutions that connect S&T's 32 IT systems—including legacy, cloud, and laboratory platforms—enabling seamless data exchange and real-time compliance reporting not available from other vendors. The incumbent also possesses specialized expertise in managing security operations for classified laboratory environments, with personnel cleared up to Top Secret/SCI and proven experience authoring ATO packages, implementing custom security controls, and supporting SCIFs and PKI programs. Additionally, the current contractor has successfully led S&T's cloud migration and Zero Trust architecture initiatives, deploying advanced security policies, DevSecOps pipelines, and automated provisioning standards tailored to S&T's unique operational and compliance needs. These technical capabilities are essential for mission continuity and cannot be readily replicated by other contractors. 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, 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. The current contractor possesses unique technical expertise in managing S&T's complex IT operations, maintenance, help

desk, and asset management services. The incumbent has engineered custom workflows within ServiceNow for ticketing, escalation, and SLA tracking, and maintains automated asset inventory processes integrated with Sunflower Asset Management System (SAMS). Their team has developed tailored scripts for patch deployment using SCCM and Red Hat Satellite, ensuring consistent compliance with DHS security mandates. The current contractor also supports specialized laboratory IT environments, including secure messaging, backup and recovery systems (Veritas NetBackup, Dell Compellent SAN), and virtualization platforms (VMware, Hyper-V). They have established protocols for rapid incident response, after-hours support, and physical asset tracking, all based on deep familiarity with S&T's operational landscape. A new contractor would lack access to these custom tools, established processes, and institutional knowledge, resulting in service disruptions, delayed incident resolution, and gaps in asset accountability and compliance. Only the current contractor can ensure uninterrupted, compliant, and efficient IT O&M support for S&T at this time. Additionally new contractor 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 obtain critical support 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.

Based on the initial market research conducted in May of 2026, Silosmashers is the only responsible source, and no other supplies or service will satisfy agency requirements because of the timing as result of recent appropriations interruptions and the contractors institution knowledge of S&T CIO operations, and the personnel possess the multidisciplinary technical expertise in areas that are central to S&T CIO.

(b) Details covering what events lead to the situation requiring use of other than full and open competition procedures including whether any portion of the work can be segregated to allow for competition.

All of the services are required for successful accomplishment of the mission. The contractor will support S&T Chief Information Office (CIO) team to meet the obligations and tasks outlined in the task order, such as, but not limited to:

- Business Management Office (BMO)- Manages IT
  - governance, compliance, project oversight, and business practices for S&T CIO.
- Information Assurance (IA) Systems Engineering- Designs

- develop and secures IT systems, supporting modernization and integration.

- Information Assurance (IA) Information Systems Security Officer (ISSO) Support
  - Maintains IT security, conducts vulnerability scans, and ensures DHS cybersecurity compliance.
- Service Delivery (SD) IT Operations & Maintenance (O&M) Support
  - Provides daily IT operations, maintenance, help desk, and asset management services.
- Service Delivery (SD) Solutions Delivery
  -Develops, upgrades, and supports IT applications and platforms, including SharePoint and ServiceNow.

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 obtain critical support to integrate innovative technology into everyday use by the DHS operational components. DHS S&T information technology (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. The sole-source extension to the incumbent will provide the service continuity that CIO requires. Additionally, the incumbent possesses the institutional knowledge of the S&T CIO operations, the personnel are experienced in multiple specialized areas that are centric to the S&T CIO.

(c) Summarize alternatives considered and why they will not work; Any gap in service would directly impact S&T's ability to support DHS missions, laboratory operations, and compliance with federal IT mandates.

A review considered several alternatives such as the use of Federal employees; however, these alternatives were not capable of providing DHS with necessary services to meet CIO needs during the required period of performance.

(d) Impact to the mission that would result if the J&A is not approved and, consequently, the product or service not provided.

The mission would be impacted negatively in many ways if this justification were not approved namely in that:

- **Continuity of Operations:**
  The contractor provides essential support for IT operations, maintenance, information assurance, systems engineering, and governance. An interruption would jeopardize mission-critical operations, including cybersecurity, network stability, and compliance with federal mandates (Federal Information Acquisition Reform Act (FITARA), Federal Information Security Management Act (FISMA), Section 508, etc.).

- **Unique Knowledge and Expertise:**
  The contractor possesses unique institutional knowledge of S&T's complex IT environment, including legacy systems, laboratory operations, and specialized security requirements. Immediate replacement would result in loss of continuity, increased risk, and inefficiency.

- **Critical Security and Compliance Requirements:**
  The contractor covers information assurance, ISSO support, and classified system operations requiring cleared personnel. The extension ensures compliance with DHS security directives and uninterrupted support for classified and sensitive systems.

- **Ongoing Projects and Deliverables:**
  Numerous IT modernization, cloud migration, and governance initiatives are underway. The extension is necessary to complete these projects and maintain progress toward S&T's strategic IT goals.

- **Avoidance of Service Disruption:**
  Any gap in service would directly impact S&T's ability to support DHS missions, laboratory operations, and compliance with federal IT mandates.

- **Security Requirements:**

  The contractor has the personnel cleared at the required levels (up to Top Secret/SCI) and is already compliant with DHS security protocols. Recruiting and onboarding new cleared personnel would take substantial time and could jeopardize compliance and operational security.

6. **Description of Efforts Made to Ensure that Offers are Solicited from as Many Potential Sources as is Practicable**

   A synopsis was posted on SAM.gov on July 7, 2026. Responses received will be addressed accordingly.

7. **Determination by the Contracting Officer that the Anticipated Cost to the Government will be Fair and Reasonable.**

The Contracting Officer has determined that the anticipated price to the Government will be fair and reasonable based on a priced analysis technique in RFO FAR 15.404-1 (b).

8. **Description of Market Research**

S&T CIO continues to analyze responses to the Request for Information (RFI) that was issued on SAM.gov for the recompete. No company other than Silosmashers has the ability to seamlessly support ongoing IT services without a significant gap for transition, onboarding, and overcoming the very steep learning curve.

During the proposed extension period, the Government will finalize the market research, solicit, and award the recompete. The responses to the RFI will aid the Government in the development of an acquisition strategy. At present, the anticipated award date of the new task order is May 2027.

9. Any Other Facts Supporting the Use of Other Than Full and Open Competition

There are no other facts supporting the Use of Other Than Full and Open Competition.

10. A Listing ofthe Sources, if Any That Expressed, in Writing, an Interest in the Acquisition

The Government received 234 different company responses to RFis 70RSAT26RFI000006, 70RSAT26RFI000009, and 70RSAT26RFIO00010, expressing interest in this requirement. .

11. A Statement of the Actions, if Any, the Agency May Take to Remove or Overcome Any Barriers to Competition Before Any Subsequent Acquisition for Supplies or Services Required

(a) The Government does not have any overly technical specifications or acquired data rights.

(b) Comprehensive market research is underway for the recompete. Detailed analysis of Request for Information (RFI) results will aid in finalizing the acquisition strategy and identifying potential sources.

(c) Market research is expected to be finalized by late July 2026 and award of the recompete is expected by May 2027.

APPROVAL:

[redacted] [redacted]

Procuring Activity Advocate for Competition Date