FSS Sole Source Justification

Office of the Director (OD)
Office of the Chief Information Officer (OCIO)

Information Security Management Support Services (ISMS)

1. IDENTIFICATION OF THE AGENCY AND THE CONTRACTING ACTIVITY.

a. Federal agency and contracting activity.

Department of Health and Human Services (HHS) | National Institutes of Health (NIH) | Office of Acquisition and Logistics Management (OALM) | Office of Logistics and Acquisition Operations (OLAO) | Specialized & Scientific Information Technology Division (SSIT)

b. Sponsoring organization.

Office of the Director (OD) | Office of the Chief Information Officer (OCIO)

c. Project Officer information.

Project Officer Name: [redacted]
Mailing Address: [redacted]
Bethesda, MD 20817
E-mail Address: [redacted]
Telephone Number: [redacted]

2. NATURE AND/OR DESCRIPTION OF THE ACTION BEING APPROVED.

a. Acquisition purpose and objectives.

Task Order 47QTCA19D00HF / 75N97021F00077 was initially competed amongst small businesses under the General Services Administration (GSA) Multiple Award Schedule (MAS) through the Special Item Number (SIN) 54151HACS, Highly Adaptive Cybersecurity Services contractor pool.

The subject services remain essential to mission execution; however, the recompete contract action has been delayed due to unforeseen circumstances outside the normal acquisition cycle. Orders and directives supporting administrative priorities - such as NIH's "Foundational IT Centralization Initiative" – required revisions to acquisition documentation, which in turn delayed the original solicitation timeline. This enterprise-wide initiative is actively expanding and restructuring the scope of IT services at the agency level and has heavily influenced the Information Security Management Support (ISMS) requirement. The Integrated Project Team (IPT) responsible for developing the recompete requirement has been unable to finalize the Requirements Package as the ISMS requirement's full expanded scope is not immediately discernable in its current state. The Foundational IT Centralization effort needs additional time to mature, ultimately allowing the ISMS requirement, among many other requirements, to manifest and settle. Otherwise, the requirement may not be fully conducive to shifting agency priorities. These circumstances were not foreseeable at the time

Source Selection Information – See FAR 2.101 and 3.104

of the original award or at the exercise of the most recent option period and are beyond the control of the NIH acquisition office administering the current task order.

As a result of these unanticipated and uncontrollable factors, it is necessary to extend the current task order to ensure continuity of mission-critical services. This extension enables NIH to maintain essential operations that impact mission-critical support provided to HHS partners. Any disruption could significantly impact OD OCIO's cybersecurity posture, potentially resulting in a range of adverse outcomes, including data loss and compliance issues. Without these services, the Government would face unacceptable delays in meeting agency requirements, severely affecting NIH's ability to deliver planning and evaluation of its cyber policy, risk management/authorization, and the evaluation and awareness of enterprise training.

The Government intends to issue a modification to extend GSA Contract # 47QTCA19D00HF, Task Order (TO) # 75N97021F00077 with [redacted] for 10 months and 15 days to prevent a lapse in service for information security management support services for OD OCIO from June 1, 2026, to April 16, 2027. The TO was awarded on a Labor Hour (LH) basis under the GSA Federal Supply Schedule Multiple Award schedule contract utilizing FAR 8.405-2(c)(3) procedures on September 30, 2021, with one (1) 12-month base period and four (4) 12-month option periods. The Option Period 04 period of performance was previously modified and reduced to May 31, 2026 (issued through Modification 01, dated 09/15/2021).

This proposed extension is to prevent a break of service while providing the Government with the necessary time to award the competitive recompete acquisition under the evolving Foundational IT Centralization framework. The length of the proposed extension is the minimum acceptable period necessary to award the follow-on contract while ensuring a continuity of services and granting a buffer for a potential transition period. The IPT anticipates solicitation release in early Q4 of calendar year 2026 and the award decision in Q1 of calendar year 2027. The new competitive requirement package will, at minimum, include revisions to requirement metrics, market research, independent government cost estimates, acquisition strategy, and solicitation enhancements.

This requirement provides support for the NIH's Information Security Program and strengthens cybersecurity safeguards for information assets, while minimizing exposure to data breaches. The NIH Information Security Program is comprised of seven major components: (1) Asset & Inventory Management, (2) Vulnerability Management, (3) Continuous Monitoring, (4) Incident Response, (5) Training & Awareness, (6) Audits & Assessments, and (7) Policies & Standards. The NIH Information Security Program proactively manages risks and provides valued services that improve the NIH information security posture and support the NIH community, culture, and mission in partnership with stakeholders in the NIH ICs, including intramural and extramural principal investigators and research staff; Clinical Center patients, physicians, nurses, and other caregivers; NIH senior management and administrative staff; and NIH IC CIOs, ISSOs, and security team members.

b. Project background.

Order Number:	47QTCA19D00HF / 75N97021F00077
Incumbent Contractor:	[redacted]
Contract Award Value:	
Total Obligated Funding:	
Period of Performance:	06/29/2021 – 05/31/2026 (One 12-Month Base Period, Four 12-Month Option Periods)

Competition: The initial award was competitively awarded

3. DESCRIPTION OF THE SERVICES REQUIRED TO MEET THE AGENCY'S NEEDS.

a. Project title.

OD OCIO Information Security Management Support (ISMS) Services

b. Project description.

As a part of the scope of the current task order, the incumbent contractor supports OD OCIO by providing continued specialized expertise to support the continued growth and evolution of OD OCIO's cyber policy, enterprise training, and enterprise risk management efforts. These support services are required to (1) reduce high risks, (2) prioritize high value assets, (3) improve protections and visibility, and (4) integrate privacy.

- **Requirement type.**

  ❑ Support services (non-research & development)
  ❑ Supplies/equipment
  ☒ Information technology (IT)

- **Type of action.**

  ❑ New requirement
  ☒ Pending Re-compete: Extension of Services under Current TO

- **Proposed contract/order type.**

  ❑ Firm-fixed-price
  ☒ Labor hour
  ❑ Indefinite delivery

- **Acquisition identification number.**

  47QTCA19D00HF / 75N97021F00077

c. Total estimated dollar value and performance/delivery period.

The period of performance will be extended by ten (10) months and fifteen (15) days (06/01/2026 – 04/16/2027) with an estimated cost of [redacted]. The total contract value is estimated to increase from [redacted] by [redacted] to [redacted].

4. IDENTIFICATION OF STATUTORY AUTHORITY AND JUSTIFICATION / RATIONALE FOR LIMITING SOURCES DEMONSTRATING THE CONTRACTOR'S UNIQUE QUALIFICATIONS TO PROVIDE THE REQUIRED SUPPLY/SERVICE.

a. Acquisition authority.

☒ This acquisition is conducted under the authority of the Multiple Award Schedule Program. Consideration of schedule contractors will be restricted to fewer than the

number required by the General Services Administration Regulation (GSAR) 538.7104-3(b)(iii): "The order should be issued on a sole source basis in the interest of economy and efficiency because it is a logical follow-on to an FSS order already issued on a competitive basis."

b. Demonstration of the proposed contractor(s) unique qualifications to provide the required supply or service.

- **Name and address of the proposed contractor(s).**

[redacted]
NAICS: 541990

- **Nature of the acquisition and proposed contractor(s) unique qualifications.**

Given the critical nature of the ongoing information security management support services, and other essential recurring support, its necessary to maintain the functionality, security, and continued support of OD OCIO's cybersecurity posture. The ISMS services are logical follow-on to an FSS order already issued on competitive basis, and the specialized services are deeply integrated with NIH's institutional processes, governance structures, and stakeholder relationships.

As the recompete requirement is still in development and the scope is being evaluated, a ten-and-half month extension of the current task order is necessary to avoid a lapse in service and to prevent the compromise of mission-essential services.

It is not feasible to award the recompete requirement within the current time frame without risking a break in critical services required by OD OCIO. Moreover, additional time is required to ensure adequate transition, in the event the re-compete award is made to a vendor other than the incumbent. The required services involve specialized expertise and unique integration with existing systems that are not available from other vendors in the time frame provided. The incumbent is embedded in NIH OCIO operations across a wide range of daily, weekly, monthly, and quarterly activities.

The ongoing Foundational IT Centralization initiative poses a high-risk period for a contractor transition. As OCIO absorbs additional IT functions and systems from across NIH ICs, the ISMS contractor must be able to adapt in real time to an evolving organizational and technical environment —responding to shifting stakeholder relationships, new system portfolios, and expanding A&A responsibilities. Only the current incumbent is capable of providing uninterrupted services at the level of quality required to ensure continuity of operations, and to avoid a break in mission-critical services.

The consequences of a break in service include, but are not limited, to -

(i) Decreased Cybersecurity Posture:

- Increased vulnerabilities as continuous monitoring, threat response, and risk management activities lapse or are degraded.
- Slower detection and response times to emerging threats across NIH's large and complex IT environment, which processes more than [redacted] of Internet traffic daily.

(ii) FISMA Compliance Failures:

- Disruption to A&A activities, risking lapses in system Authorizations to Operate (ATOs) for OCIO and IC information systems.
- Failure to meet mandatory annual security awareness and role-based training requirements for NIH staff, resulting in FISMA non-compliance.
- POA&M tracking failures, increasing NIH's enterprise risk posture and exposure to audit findings from OIG, GAO, and HHS.

(iii) Operational Degradation:

- Loss of real-time cybersecurity dashboards and metrics used by NIH CIO and CISO for decision-making.
- Disruption to the IT Security Service Desk, leaving OCIO staff and IC personnel without timely responses to information security and privacy inquiries.
- Loss of management and maintenance of NIH's Information Security Program Wiki, SharePoint, and communication platforms, degrading program-wide information sharing.

(iv) Risk to Foundational IT Centralization:

- A contractor transition during active centralization would significantly increase risk to OCIO's ability to absorb new IC functions, as the ISMS contractor plays a direct role in coordinating with IC CIOs and ISSOs and supporting their security compliance activities.

(v) Financial and Transition Costs:

- Duplicative costs associated with onboarding a new contractor into a rapidly evolving environment, including knowledge transfer, system access provisioning, and ramp-up time that cannot be recovered.
- Potential fines and recovery costs associated with security incidents or compliance failures arising from a gap in service.

The incumbent contractor possesses the institutional and operational knowledge needed to fulfil the requirements in the Statement of Work (SOW) and has consistently provided the qualified personnel to effectively meet those requirements. Given the current status of the recompete task order, and the potential transition to a new contractor, significant risks are present, including duplication of cost not recoverable through competition, mission degradation and the compromise of OD OCIO’s cybersecurity posture.

Source Selection Information – See FAR 2.101 and 3.104

The incumbent contractor has demonstrated a high level of expertise and familiarity with OD OCIO's Information Security systems and given their proven track record of successful project delivery, they are the best qualified vendor to maintain continuity of services during this interim period until a competitive task order is awarded. The extension will allow sufficient time to conduct a proper, FAR compliant competitive acquisition without compromising the integrity of OD OCIO's mission-critical services.

The information above reinforces that it is imperative for work to continue under the current TO with the incumbent contractor in the interest of economy and efficiency, as they are uniquely positioned to provide the required services at the necessary level of quality within the limited time frame available.

5. **DETERMINATION BY THE ORDERING ACTIVITY CONTRACTING OFFICER THAT THE ORDER REPRESENTS THE BEST VALUE.**

By placing an order against the GSA MAS contract using the procedures in GSAR Subpart 538.71, the ordering activity Contracting Officer has concluded that the award of a ten-month fifteen-day extension to [redacted] represents the best value to the Government and results in the lowest overall cost alternative (price, administrative costs, and security risks, etc.) to meet the Government's immediate needs. The Contracting Officer and the OCIO Project Officer will conduct a price evaluation by assessing whether the proposed level of effort, labor mix, and labor hours are appropriate for the work to be performed, and to determine whether the total price is fair and reasonable.

The incumbent contractor's pricing was determined to be fair and reasonable as determined by FAR 8.404(d) and they have historically provided discounts in addition to their GSA MAS rates. The incumbent contractor will be encouraged to propose additional discounts for ten-month fifteen-day extension.

6. **DESCRIPTION OF THE MARKET RESEARCH CONDUCTED AMONG SCHEDULE HOLDERS AND THE RESULTS OR A STATEMENT OF THE REASON MARKET RESEARCH WAS NOT CONDUCTED.**

The Government intends to conduct Market Research in accordance with Revolutionary FAR Overhaul (RFO) Part 10 as a part of the fully competitive TO recompete.
The Government intends to publish a limited-sources justification notice, within 14 days after placing the order, to SAM.Gov for a minimum of 30 days in accordance with GSAR 538.7104-3(b)(3)(i).

7. **OTHER FACTS SUPPORTING THE JUSTIFICATION.**

None.

8. **STATEMENT OF ACTIONS TO REMOVE OR OVERCOME BARRIERS THAT LED TO THE RESTRICTED CONSIDERATION BEFORE ANY SUBSEQUENT ACQUSITION FOR THE SUPPLIES OR SERVICES IS MADE.**

The Government will only solicit the incumbent contractor for the current TO extension under this GSA Federal Supply Schedule Multiple Award Schedule contract, to extend the existing TO for ten months and fifteen days as no reasonable alternatives exist for this requirement. No other firm can provide the necessary services at the requisite level of expertise within the time frame

required and the extension should be issued on a sole source basis in the interest of economy and efficiency because it is a logical folow-on to an FSS order already issued on a competitive basis.

The Government is actively working on the subsequent TO re-compete, which is currently in the requirements development phase. It is anticipated that a competitive award will be in place upon expiration of the current TO's ten-month fifteen-day extension. OD OCIO's technical staff continually monitors the market and evaluates services on an ongoing basis that would potentially improve their existing platforms. As Foundational IT Centralization initiatives mature, the technical staff will monitor the marketplace and re-evaluate the requirement to see if other solutions can be utilized to enhance competition.

[Certification & Signatures Follow]

9. PROGRAM OFFICE CERTFICATION:

This is to certify that the portions of this justification that have been developed by the undersigned program office personnel, including supporting information and/or data verifying the Government's minimum needs or requirements, or other rationale for limited sources, are accurate and complete.

Official	Name & Title	Signature & Date
COR	[redacted] Contracting Officer's Representative OD OCIO	[redacted]
Program Officer	[redacted] Acting Deputy CISO OD OCIO	[redacted]
Head of the Sponsoring Program Office	[redacted] Acting CISO OD OCIO	[redacted]

10. CONTRACTING OFFICER CERTIFICAITON:

This is to certify that the justification for the proposed acquisition has been reviewed and that to the best of my knowledge and belief the information and/or data provided to support the rationale and recommendation for approval is accurate and complete.

Official	Name & Title	Signature & Date
Contracting Officer	[redacted] Contracting Officer OALM OLAO SSIT	[redacted]

Contracting Officer's Immediate Supervisor	[redacted] Section C Chief OALM OLAO SSIT	[redacted]
Contracting Office's Division Director	[redacted] Director OALM OLAO SSIT	[redacted]

11. CHIEF OF THE CONTRACTING OFFICE AND HEAD OF THE CONTRACTING ACTIVITY SIGNATURE(S):

Official	Name & Title	Signature & Date
Head of the Contracting Activity	[redacted] Head of Contracting Activity / Director OM OD OALM	[redacted]

12. COMPEITITON ADVOCATE SIGNATURE:

Official	Name & Title	Signature & Date
Competition Advocate	[redacted] Director of Research Integrity NIH	[redacted]