SOURCES SOUGHT NOTICE
Information Technology Support Services (ITSS)
Executive Secretariat (S/ES) – ExecTech
U.S. Department of State

This is a Sources Sought Notice as outlined in FAR 15.201(d). The purpose of this notice is to accomplish market research pursuant to Federal Acquisition Regulation (FAR) Part 10, and to identify qualified and experienced 8(a) businesses capable of and interested in providing the services described herein. The purpose of this notice is to identify qualified and experienced vendors capable of providing Information Technology Support Services (ITSS) for the U.S. Department of State, Executive Secretariat (S/ES), ExecTech Office.

This notice is issued solely for information and planning purposes and does not constitute an Invitation for Bid (IFB), Request for Quotation (RFQ), or Request for Proposal (RFP). Additionally, there is no obligation or commitment on the part of the Government to acquire any products or services described within this notice now or in the future. The Government does not intend to award any contract(s) based solely on the submission of this notice. Respondents are advised that the Government will not pay for information submitted in response to this notice, nor will it compensate respondents for any costs incurred in the development/furnishing of a response. **The Government will not entertain telephone calls or questions for this notice**. Please note that a decision not to submit a response will not preclude a vendor from participating in any future solicitation.

Information Technology Support Services are currently being provided by Improvix Technologies Inc, 8(a) program participant, under Blanket Purchase Agreement (BPA) 19AQMM19A0208. The remaining 2 active task orders are due to expire May 15, 2026. The Government intends to compete the Department of State Information Technologies Support Services (ITSS) BPA under the 8(a) program. The intent is to award a single BPA, with ceiling between $100Mil to $150Mil for a period of five (5) years (a one-year base period and four (4) one-year options).

1. BACKGROUND

The Executive Secretariat (S/ES) serves as the Secretary of State's principal mechanism for policy coordination, crisis management, and authoritative communication across the Department of State and the interagency community. Within S/ES, ExecTech provides mission-critical, executive-level IT services supporting senior leadership.

ExecTech operates a 24x7x365 environment across classified and unclassified systems, delivering white-glove IT services that support global travel, crisis response, and continuity-of-government operations.

The majority of ExecTech's ITSS services include:

ExecTech primarily focuses on enabling executive leadership decision-making and mission execution through secure, reliable, and always-available information technology services. These services support both foreign policy and administrative operations in a high-tempo, global environment, ensuring the Secretary of State, Department Principals, and Executive Secretariat leadership can operate without interruption. ExecTech emphasizes responsiveness, discretion, and operational resilience to support crisis response, international travel, continuity-of-government operations, and senior-level engagements.

ExecTech is committed to building, operating, and sustaining a robust, secure IT infrastructure across classified and unclassified environments. This infrastructure enables executive communications, collaboration, mobility, and secure information flow across multiple locations and enclaves. In addition, ExecTech provides dedicated, on-site deskside support to ensure real-time, hands-on assistance for executive users and mission-critical staff support that cannot be performed remotely due to security, system integration, and operational requirements. ExecTech also prioritizes strengthening the technical readiness of its supported workforce through standardized onboarding, executive user training, documentation, and just-in-time, in-person support tailored to senior leaders and high-tempo operations.

A core element of ExecTech's mission involves integrating security, risk management, and compliance into all technology services. ExecTech achieves this by embedding cybersecurity, privacy, and secure-by-design principles into system engineering, service delivery, and operations. ExecTech works closely with Department stakeholders to ensure compliance with federal and Department IT, cybersecurity, records management, and accessibility requirements, while continuously modernizing systems to reduce risk and technical debt.

Additionally, ExecTech oversees and supports enterprise IT governance, portfolio planning, and mission operations for S/ES. This includes aligning IT investments with mission priorities, supporting executive governance forums, managing vendor performance, and enabling Congressional, litigation, and records-management support. ExecTech collaborates across bureaus to ensure a cohesive, accountable, and mission-aligned approach to executive IT services.

ExecTech ITSS Functional Areas

ExecTech ITSS services are organized across the following functional areas:

1. **Front Office Operations**
   Provides executive-level administrative, programmatic, and operational IT support, including governance coordination, resource planning, staffing transitions, executive reporting, and continuity of operations.

2. **Executive Support Services**
   Delivers white-glove customer support, executive communications, mobile and flyaway kit support, VTC services, account and asset lifecycle management, and direct engagement with senior leaders across all environments.

3. **Service Delivery & Engineering**
   Designs, integrates, secures, and operates networks, infrastructure, applications, automation, and digital platforms, using Agile and modern engineering practices to support mission execution and system reliability.

4. **Cybersecurity, Risk & Mission Operations**
   Ensures continuous authorization, cybersecurity risk management, compliance, IT governance, financial oversight, records and knowledge management, Congressional and litigation support, and overall operational integrity.

2. SCOPE / REQUIRED CAPABILITIES

As ExecTech's mission, technology footprint, and operational tempo have expanded in scope, complexity, visibility, and criticality, the Executive Secretariat (S/ES) requires industry partners capable of delivering enterprise-scale, mission-critical Information Technology Support Services (ITSS). The operating environment demands secure, resilient, and highly responsive IT services that support executive leadership, crisis response, global travel, continuity-of-government operations, and sustained operations across both classified and unclassified environments.

To meet these requirements, ExecTech seeks vendors with demonstrated experience providing integrated advisory, engineering, operational, cybersecurity, and governance capabilities, including but not limited to the following:

Ad Hoc Advisory & Executive IT Advisory Services

- Experience providing on-demand advisory support to senior executive IT leadership within a federal environment, including advising on operational, technical, and governance challenges unique to executive-level IT support.

- Demonstrated understanding of federal budget cycles, acquisition processes, security clearance requirements, and inter-bureau coordination mechanisms impacting IT services.

- Experience advising on IT service delivery models, executive support frameworks, and operational IT strategies aligned with federal policies, Department of State standards, and enterprise architecture.

Special Projects & Surge Operations

- Experience executing special projects and surge operations requiring familiarity with the Department of State operational environment, including diplomatic security requirements, executive travel support, classified communications, and crisis response.

- Ability to rapidly scale staffing, technical capabilities, and operational support to meet time-sensitive, high-visibility mission demands.

Quality Control, Performance Management & Continuous Improvement

- Experience developing and implementing quality control and performance management processes for IT services supporting executive or mission-critical operations.
- Ability to define, track, and report service performance metrics, customer satisfaction indicators, and operational risk measures.
- Experience supporting inspection readiness, audits, and continuous service-improvement initiatives.

Customer Engagement, Communications & Training Support

- Experience delivering customer-focused communications supporting executive IT services, including service updates, briefings, dashboards, and executive-level reporting.
- Ability to develop and maintain user documentation, job aids, and training materials tailored to senior leaders and mission-critical staff.
- Experience applying UI/UX-informed approaches to improve usability, accessibility, and adoption of executive-facing digital tools and platforms.

Enterprise Systems Administration & Directory Services

- Demonstrated experience managing Active Directory (AD) architectures, including user and group management, organizational units (OUs), domain controllers, forests, and trust relationships.
- Experience administering Windows and Linux server environments, including system hardening, patching, performance monitoring, and lifecycle management.
- Familiarity with storage virtualization technologies and integration with platforms such as VMware and Hyper-V.

Network Engineering & Infrastructure Operations

- Strong understanding of TCP/IP, DNS, DHCP, and the ability to troubleshoot complex network issues across distributed environments.
- Experience configuring and managing network security controls, including firewalls, routing, segmentation, and access controls.
- Ability to design, operate, and secure network infrastructure supporting both classified and unclassified systems.

Security Engineering, Backup & Data Protection

- Experience implementing security controls to protect systems, data, and communications, including firewall management and data-protection mechanisms.
- Demonstrated capability designing and implementing backup, archiving, and recovery strategies, including routine recovery testing to ensure operational resilience.
- Proficiency with SAN, NAS, and DAS storage solutions, including performance optimization and capacity planning.

Automation, Scripting & Configuration Management

- Experience using scripting languages (e.g., PowerShell) to automate administrative, operational, and compliance-related tasks.
- Familiarity with configuration management and automation tools to improve consistency, reduce manual effort, and enhance system reliability.

Cloud Engineering & DevOps

- Demonstrated experience deploying and managing cloud resources and services within major cloud service providers (e.g., AWS, Azure, Google Cloud).
- Experience with CI/CD pipelines and infrastructure-as-code (IaC) solutions (e.g., Terraform, CloudFormation).
- Understanding of cloud networking concepts, including virtual networks/VPCs, subnets, routing, and security groups.
- Capability to monitor cloud performance, optimize resource utilization, and manage operational costs in accordance with federal and Department policies.

Mission-Critical Application & Platform Support

- Experience supporting and maintaining mission-critical applications, including monitoring system uptime, performance, and responsiveness.
- Familiarity with Department-specific systems such as SPB/ Cascades, Microsoft Power Apps, and other apps including applying security patches, performing system health checks, and implementing data backup and recovery procedures to protect sensitive information.

Video Teleconferencing (VTC) & Executive Communications

- Demonstrated experience supporting enterprise and executive-level Video Teleconferencing (VTC), including managing multiple bridge types, classified and unclassified sessions, and high-visibility executive engagements at TS Level.
- Ability to provide just-in-time, on-demand VTC support for senior leadership, including troubleshooting and cross-stakeholder coordination.

Cybersecurity, Risk Management & Compliance

- Demonstrated capability supporting cybersecurity risk management, continuous authorization, and incident response in accordance with FISMA, NIST, FedRAMP, and Department of State policies.
- Ability to demonstrate compliance with 19 FAM 101.1-3(A) (Primary Cyber Laws, Regulations, and Executive Orders), including reporting through mechanisms such as the ECISO Cybersecurity Scorecard.
- Experience addressing and remediating findings identified by the Bureau of Diplomatic Security’s Cyber Threat Analysis Division (DS/CS/CTA), including remediation of vulnerabilities identified during FISMA High-Value Asset (HVA) assessments.
- Demonstrated organizational experience conducting Assessment and Authorization (A&A) activities in accordance with NIST SP 800-53 Revision 5, including experience supporting Department systems using tools such as Archangel.
- Ability to support continuous monitoring, vulnerability management, audit readiness, and inspection activities across multiple systems and environments.

General Scope Requirements

Vendors responding to this Sources Sought Notice should demonstrate the ability to:

- Strategically manage complex IT infrastructure, systems, and security operations within the federal government’s regulatory and operational framework, including classified and sensitive but unclassified environments.
- Provide integrated engineering, operations, automation, cybersecurity, and advisory support aligned with executive-level mission requirements.
- Support high-availability, high-visibility systems with minimal tolerance for downtime or service degradation.
- Oversee intake, prioritization, lifecycle management, financial tracking, and performance reporting for IT services and initiatives.

- Develop, implement, and maintain quality control, compliance, and continuous-improvement processes aligned with Department-specific requirements.
- Deliver technically strong solutions while maintaining a customer-focused, service-oriented approach appropriate for executive and mission-critical environments.

3. SECURITY REQUIREMENTS

This requirement requires access to classified information. Therefore, the interested offerors, including all entities which comprise a joint venture must possess a Defense Counterintelligence and Security Agency (DCSA) active Top-Secret Facility Clearance Level (FCL) and all personnel shall maintain up to Top-Secret clearances, depending on the role as outlined in the Labor Categories. Uncleared individuals specifically authorized by the COR may perform on-site in DOS facilities, only on unclassified portions of the requirement and/or in areas not requiring cleared access but must still be processed for DOS personal identification cards (badges) in accordance with the DOS Personal Identification Card Issuance Procedures.

4. INSTRUCTIONS

4.1 Responses

Vendor evaluations will assess if a vendor is capable by examining their submission for evidence of their ability to meet all performance objectives. Mere assertions of capability are inadequate; vendors must provide tangible evidence. Responses to this notice should be and limited to a maximum 20 pages in total. Submissions should be in either Microsoft Word Document (.doc or .docx) or Portable Document Format (.pdf) and sent via the provided email address. Submissions must include the following sections: Company Profile, and Recent/Relevant Experience.

4.1.1 Company Profile, to include:

1. The Company Profile section requires that a viable interested party showcases the company's ability to meet both the work/performance objectives and the customer’s needs. It is crucial that the specific work/performance objectives are directly addressed. Moreover, demonstrating capability includes providing examples of prior implementations of similar or greater scope and complexity. This includes furnishing relevant, applicable examples of previous work or solution implementations, accompanied by client points of contact.

2. General Business Information, completing the following table:

Company Name:	
8(a) Program Graduation Date:	
8(a) Type:	*Example: Tribal; Regular, JV*
Company Point-of-Contact:	
Address:	
Email:	

Phone:	
UEI Number:	
Cage Code:	
Socio-economic Status	*Example: Small Business, Small Disadvantaged Business; HUBZone; Economically Disadvantaged Woman-Owned; Service Disabled Veteran Owned; 8(a)*
GSA Schedule Contracts or other GWAC (if applicable and number.):	
GSA Expiration Date:	
Current CMMI Level, ISO certifications, or Other industry certifications:	
Are you capable of meeting ***all*** of the technical requirements outlined in the Scope above?	*Yes/No*
Will you be sub-contracting or teaming any of the work outlined in the Scope above? If so, what percentage and what are the companies' socioeconomic statuses?	

4.1.2 Recent/Relevant Experience, to include:

-

Capabilities: Business

1. History and overview of your firm, indicating the general areas of focus for your business, and your years of relevant experience as a prime contractor. Please highlight where experiences are recent, in support of U.S. Government programs of similar scope and complexity.

2. Specific experience and qualifications relevant to the suite of services and capabilities that the program requires, as outlined in scope included above. For each objective provide:

   a. Brief descriptions of successful recent projects similar in scope and complexity, citing references

   b. Operating models implemented and strategies employed to deliver these services effectively and efficiently under performance-based arrangements

5.0 Point of Contact

Responses must be submitted as either a Microsoft Word Document (.doc or .docx) or Portable Document Format (.pdf) to the following e-mail addresses: Contracting Officer, Jeannie R. Mays at maysjr@state.gov and Contract

Specialist, Earl A. Brown at brownea1@state.gov. Responses are due no later than Noon EST February 13, 2026. To the maximum extent possible, submit Non-Proprietary Information. All information received in response to this notice that is appropriately marked "Proprietary" will be handled accordingly.