General Services Administration
Federal Acquisition Service
Technology Transformation Services
1800 F St NW | Washington, DC | 20405

Technology Transformation Services (TTS)
Next-Generation IT Solutions (NEXT)
Blanket Purchase Agreements (BPAs)

Performance Work Statement

1.0 Background

The General Services Administration (GSA) Federal Acquisition Service (FAS) Technology Transformation Services (TTS) helps agencies make their services more accessible, efficient, and effective with modern applications, platforms, processes, personnel, and software solutions.

The TTS Technology Acquisition Division (TechAcq) anticipates establishing a suite of Blanket Purchase Agreements (BPAs), based on the Support Areas (SAs) listed in section 2.0 below, to support all TTS programs, allowing for efficient and innovative modern IT solution procurements. These BPAs will be a mix of single-award and multiple-award.

2.0 Support Areas

The scope of the BPAs encompasses modern, secure, and user-centric digital and ITS services for TTS programs. The intent is for the BPA SAs to allow for cross-functionality of services between SAs. However, BPA/SA usage will be selected by the Government based on the scope of the preponderance of the services required.

BPAs are anticipated to be awarded for the following SAs:

SA1. DevSecOps & Secure Modern Development

Purpose: Provide secure software development and delivery support across programs using an integrated Developer, Security, and Operations (DevSecOps) mindset.

Key Services Covered:

- Modern application engineering with DevSecOps toolchain
- Continuous integration/continuous delivery (CI/CD) automation
- Infrastructure and software testing and quality assurance
- Secure code practices, threat modeling, vulnerability scanning, automated testing for security, performance, and accessibility
- Containerization, microservices, and cloud-native application support
- Infrastructure as Code (IaC), platform engineering, and automated compliance controls
- Systems operations and maintenance, data integrity, reporting, and interoperability support
- Performance, monitoring, and systems observability
- Application support, defect resolution, patching, and performance optimization
- User support enablement, system enhancements, incremental modernization, and integration with legacy and third-party systems
- Data engineering, analytics, visualization
- Planning, collaboration, portfolio management, and documentation
- Software supply chain security and open source governance
- Secrets management and key rotation
- Cloud Security Posture Management (CSPM)

Why it matters: Modernizing federal digital services depends on secure, continuous and rapid delivery of high-quality software. High-quality, maintainable digital products and data solutions delivered iteratively and reliably.

2. Digital Services & Experience Design & Delivery

Purpose: Provide human-centered design and digital experiences for public-facing and internal users.

Key Services Covered:

- Human-centered design, user research, and journey mapping
- User Experience / User Interface (UX/UI) design and design systems
- Information architecture and content strategy
- Prototyping, modeling, and usability testing
- Accessibility engineering and compliance (e.g., Section 508, WCAG)
- Multichannel experience design (web, mobile, forms, tools)
- Iterative design and product improvement throughout agile delivery
- API and shared service integration support
- Customer service technology support and integration
- IT Program Support
- Business Process Operations
- Service blueprinting and service delivery model design
- Service analytics, performance measurement, and continuous user insights

Why it matters: Intuitive, efficient, accessible, and equitable digital services that meet real user needs.

3. Cloud, Infrastructure, & Cybersecurity Services

Purpose: Enable secure, scalable, resilient, and cost-effective cloud and infrastructure modernization through engineering-led cybersecurity, technical risk management, and operational excellence across government partners.

Key Services Covered:

- Cloud migration planning, engineering, execution, operations, and optimization
- Cloud and hybrid infrastructure engineering and administration, including IaaS, PaaS, networking, storage, and platform services
- Secure system, infrastructure, and enterprise architecture

- Technical security engineering and control implementation for cloud, infrastructure, and shared platforms
- Secure infrastructure, platform, and operational support for AI, agentic, and data lake/data warehouse environments, including data pipelines, workload integration, access control, monitoring, scalability, and risk-informed implementation
- Identity, credential, and access engineering, including authentication, authorization, federation, privileged access, and zero trust implementation
- Keys, credentials, certificates, and secrets management
- Technical risk analysis, threat-informed design, and risk mitigation planning
- Secure configuration management, hardened baselines, and automated policy enforcement
- Continuous monitoring, logging, alerting, observability, and operational security telemetry
- Vulnerability management, patch management, threat detection, incident response, and remediation support
- Platform engineering and shared services operations, including hosting, container orchestration, and secure platform administration
- Resilience, scalability, performance engineering, backup, continuity of operations, and disaster recovery support
- Systems, network, platform, and infrastructure operations and maintenance support
- Infrastructure automation, Infrastructure as Code, policy-as-code, and secure platform provisioning
- Cost optimization, resource management, and cloud financial operations support
- Security assessment and authorization support for technically implemented, testable, and sustainable controls

Why it matters: Agencies need teams that can support the rapid deployment of technology and systems while managing risk through sound architecture, automation, technical control implementation, and continuous operations.

4. Digital Identity & Fraud Protection

Purpose: Provide specialized technical, security, and operational support as a government-wide digital identity service. Prevent, detect, investigate, and mitigate fraud, abuse, and malicious activity across digital systems, programs, and services.

Key Services Covered:

- Identity verification (IdV) engineering and integration support
- Authentication, authorization, and federation services
- Platform reliability, scalability, and performance engineering
- Security engineering, fraud detection, and threat mitigation
- Partner agency onboarding, integration support, and tooling
- Compliance with privacy, security, and identity standards
- Entity identity validation and authorization
- Legal validation and authorization of individuals and entities
- Entity ownership and control verification
- Data quality, integrity, and revalidation
- Fraud detection and analysis design and implementation
- Data analysis, anomaly detection, and risk scoring
- Threat mitigation and prevention tools within digital services and workflows
- Bot detection, account abuse prevention, and automated misuse mitigation
- Identity, eligibility, and transaction risk assessments
- Vulnerability assessment
- FedRAMP Authorization / Authorization to Operate (ATO)

Why it matters: Secure digital identity, Zero Trust architecture, fraud reduction, and improved access to government services. Fraud reduction, improved service delivery and access to Government services, strengthens public trust.

5. Artificial Intelligence Strategy & Implementation

Purpose: Responsible design, development, deployment, and operation of AI-enabled capabilities.

Key Services Covered:

- AI and machine learning strategy development, roadmaps, and use-case prioritization
- Responsible AI governance, risk management, testing, and ethics frameworks
- Development, integration, and optimization of AI/ML solutions
- Data readiness, data quality, model training, evaluation, and lifecycle management
- Natural language processing, computer vision, and predictive analytics
- Virtual AI agent support and technology integration
- FedRAMP Authorization / Authorization to Operate (ATO)
- AI testing, validation, red-teaming, and operational readiness assessment

- MLOps, LLMOps, model deployment, monitoring, drift detection, and lifecycle operations
- Continuous evaluation (Bias, robustness, explainability, and performance validation), drift detection
- Human oversight, review workflows, escalation paths, and decision governance
- AI-ready data architecture and pipelines
- Logging, auditability, traceability, and performance monitoring for AI systems
- AI integration with enterprise platforms, APIs, mission workflows, and user-facing services

Why it matters: Secure, ethical, and effective AI capabilities that enhance mission delivery while managing risk.

*All implementations must follow GSA Order: Accelerating Responsible Use of Artificial Intelligence at GSA and the GSA Artificial Intelligence Compliance Plan.

3.0 Type of Contract

All resulting BPAs will allow for all contract types described in FAR Part 16, except for Cost-Reimbursement call orders. The contract type selection will be determined and documented at the BPA call order level.

4.0 Period of Performance

Each BPA will include a five-year ordering period. BPA call orders may be up to five years in length and may extend up to five years past the expiration of the BPA ordering period, provided the GSA Multiple Award Schedule (MAS) and Alliant 3 contract is in effect and has remaining option periods available.

5.0 Estimated Value

The Government estimates that the volume of all call orders across all BPAs over the five-year ordering periods will be approximately $700M; however, this is only an estimate, not a guarantee of work. The Government reserves the right to exceed or fall short of the estimated value in order to meet TTS priorities, customer agency needs, and changing demands of the Administration. The BPAs will not obligate any funds, and there is no limit to the dollar value of the call orders or number of call orders issued under each BPA.

6.0 Call Orders

Tasks & Deliverables:
Tasks and deliverables will be outlined in each BPA call order.

Ordering Procedures:
Under the multiple-award GSA Multiple Award Schedule (MAS) BPAs, the Government reserves the right to solicit from as many BPA holders as practicable for call orders above the Simplified Acquisition Threshold (SAT) in accordance with GSAR 538.7104-1(a)(4)(ii)(B). When applicable, sole-source justifications will be determined at the call order level in accordance with GSAR 538.7104-3.

Under the Alliant 3 Governmentwide Acquisition Contract (GWAC) BPA, sole-source justifications will be determined at the call order level in accordance with FAR 16.507-6 when applicable.

Order Level Materials (OLMs):
Following the procedures at GSAR 538.7104-2, OLMs / OLM Special Item Numbers (SINs) may be included at the call order level for the GSA MAS BPAs.

7.0 On/Off Ramping

This section only applies to the multiple-award BPAs.

On-Ramp Procedures:
The Government will review BPA performance and requirements on a regular basis (at least annually) and determine the necessity of on-ramping for the multiple-award BPAs. The Government reserves the right to announce and issue a new solicitation for the purpose of adding additional contractors to expeditiously meet increasing needs and increase competition. The Government may implement on-ramp procedures at any time by reopening the competition and utilizing the same basis of award established in the initial solicitation. Any resulting BPA(s) awarded will include the same terms and conditions as the current BPAs, and the period of performance term for any new awards is coterminous with the existing term for all other contractors. Immediately upon on-ramping, the contractor is eligible to submit a quote in response to any call order solicitation and receive call orders with the same rights and obligations as any other contractor.

Off-Ramp Procedures:

The Government reserves the right to implement off-ramp procedures, which would result in the removal of BPA holders. The criteria for off-ramping may include, but is not limited to, BPA holders not quoting on call order request(s), not having at least one call order award, no longer maintaining an active GSA MAS contract or required SIN(s), and/or performing unsatisfactorily on call orders. If implemented, off-ramp procedures will remove BPA holders by not exercising the next available ordering period option or canceling the BPA. Removal from the BPA applies only to eligibility for future orders and does not impact the performance or validity of any existing awarded orders.

8.0 Limitations on the Release of Contract Award Information to the Public, News Media, and Members of Congress

General

The Contractor, its affiliates, agents, subcontractors, and respective employees:

Must not issue press releases or provide other information to the public, news media, or Members of Congress regarding any TTS contract award or their services under this BPA or any call order issued under it, without prior written authorization by the Contracting Officer (CO) specified in the contract.

Must cooperate with the Stakeholder Engagement Team and CO in releasing unclassified information to the public, news media, and Congress regarding TTS policies, programs, and activities directly related to the contracting effort outlined herein.

Must notify the CO or Technology Acquisition Division TechAcq) immediately upon receipt related to activities or situations that may attract regional or national news media attention and of non-routine inquiries from national news media relating to the effort performed under the contract, upon immediate discovery.

Must not issue or sponsor advertising or publicity that states or implies that the federal government agency endorses, recommends, or prefers the Contractor's services.

Must not use the agency’s logo, or other material, without agency permission.

Guidance

Contractors must submit all requests for press release approval to the CO specified in the contract. Requests for approval must identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor must submit requests to the CO at least 15 business days before the proposed date for release. The CO will review the press release and forward it to the Stakeholder Engagement Team for their concurrent review and approval. Contractors may proceed with issuing a press release once written approval has been granted by the CO. Final approval may take up to ten business days to be granted.

The Contractor agrees to include a similar requirement process in each subcontract under this contract. Subcontractors must submit requests for authorization to release through the prime contractor to the CO.

9.0 TTS Transparency Policy

BPA holders are advised that TTS reserves the right to publish documents associated with the BPAs and subsequent call orders on publicly-available websites. TTS reserves the right to publish relevant information that is not confidential or proprietary in nature, but will not publish any evaluation sensitive information that would otherwise implicate procurement integrity concerns.

Upon award of the BPAs, TTS may publish certain non-source-identifying data (e.g. the number of bids, the mean price, the median, and the standard deviation of price). During the performance of the BPAs and subsequent call orders, TTS may similarly publish data related to project management (e.g. user stories, milestones, and performance metrics), price, and top-line spending data.