U.S. Department of State

Evolve

DRAFT
SOLICITATION

(This page is intentionally left blank.)

Table of Contents

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

TBD

SECTION C – STATEMENT OF WORK

C.1 General

C.1.1 Objective

Information Technology (IT) support services represent a significant portion of the Department of State (DOS) IT budget. The primary goal of this acquisition is to establish a suite of indefinite-delivery indefinite-quantity contracts for IT support services that will enable DOS business and program units to accomplish their mission objectives.

EVOLVE is intended to provide information technology (IT) solutions and services as defined in FAR 2.101(b), clarified in the Clinger-Cohen Act of 1996, and as amended further refined in Federal IT Acquisition Reform Act of 2014.

The acquisition and resulting multiple award contracts will collectively be referred to as EVOLVE and are designed to offer a broad range of services, solutions and contract types to fulfill the majority of component and departmental IT service needs. This Statement of Work is comprised of five comprehensive pools. Specific requirements will be further identified and defined at the task order level.

C.1.2 Scope

The Contractor shall provide the full range of IT services, technical and management expertise, and solution-related enabling products in one or more of the pools to meet the mission needs of the Department of State. As identified in individual Task Orders, information technology solutions/capabilities will support DOS on a world-wide basis. The Contractors shall furnish the necessary personnel, materials, equipment, facilities, travel, and other services required to satisfy the ordered IT capabilities and solutions. While the Statement of Work (SOW) identifies five pools, the suite of resulting contracts is intended to satisfy the full range of IT related requirements. The scope of each individual IDIQ contract will be based upon the pools for which the Contractor proposed and is selected. With the pace of change it is impossible to anticipate how IT requirements and individual programs will evolve over the life of the contracts. It is intended that the EVOLVE contract remains current and continues to provide the full range of IT capabilities/solutions and emerging technologies throughout its life. The Contractor shall provide solutions for one or more of the following functional categories with specific tasks to be set forth in the TOs:

(1) IT Management
(2) Network Services
(3) Cloud and Data Services
(4) Application and Development
(5) Customer and End User Support Services

C.1.3 Contract and Task Order Management

Contract and TO management is mandatory for all task orders placed under the EVOLVE contract. The objective of contract and TO management is to provide the program management, project control and contract administration necessary to manage a high volume, multiple contract type TO process for a large, diversified team so that the cost, schedule and quality requirements of each order are tracked, communicated to the government, and ultimately attained. The use of commercially available automated tools and the application of expertise on processes and metrics that support task order management are encouraged to achieve the above objectives. The objective of the tools is to provide quicker access, improved accuracy, and enhanced accessibility for Contractors/clients, real-time monitoring of status/deliverables, tracking the quality of work products and gauging overall customer satisfaction.

C.1.4 Cybersecurity

Cybersecurity is mandatory for all task orders placed under the Evolve contract. The objective of the cybersecurity requirement is to ensure that all task orders placed under the Evolve IDIQ not only comply with DOS standards but go above and beyond those requirements to consider how to make DOS systems more resilient and secure in the face of continuously changing threats. The following are the current cybersecurity standards, frameworks and policies that will apply at the task order level as applicable. The list is not all inclusive and is subject to change:

Federal Information Processing Standards Publications (FIPS Pub)	
Security Requirements for Cryptographic Modules	FIPS Pub 140-2
Standards for Security Categorization of Federal Information and Information Systems, February 2004	FIPS Pub 199
Minimum Security Requirements for Federal Information and Information Systems, March 2016	FIPS Pub 200
Personal Identity Verification of Federal Employees and Contractors," August 2013	FIPS Pub 201-2

National Institute of Standards and Technology (NIST)	
Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, June 10, 2014	NIST SP 800-37
Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015	NIST SP 800-53 Rev. 4
A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008	NIST SP 800-116
Digital Identity Guidelines, June 2017	NIST SP 800-63-3, 800-63A, 800-63B, 800-63C
Guidelines for Derived PIV Credentials, December 2014	NIST SP 800-157
Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012	NIST SP 800-164
Draft National Institute of Standards and Technology Interagency Report - Mobile, PIV, and Authentication, March 2014	NISTIR 7981

Office of Management and Budget (OMB)	
Managing Federal Information as a Strategic Resource," July 28, 2016	OMB Circular A-130
Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011	OMB memorandum M-11-11
Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008	OMB Memorandum
Transition to IPv6, September 28, 2010	OMB Memorandum
Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006	OMB Memorandum M-06-18
E-Authentication Guidance for Federal Agencies, December 16, 2003	OMB Memorandum 04-04

Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005	OMB Memorandum 05-24
Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007	OMB Memorandum M-07-16
Implementation of Trusted Internet Connections (TIC), November 20, 2007	OMB Memorandum M-08-05

Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008	OMB Memorandum M-08-23
Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents August 27, 2021	OMB Memorandum M-21-31

Security Policies	
"Trusted Internet Connections (TIC) Reference Architecture Document, Federal Interagency Technical Reference Architectures, Department of Homeland Security, (https://www.doi.gov/sites/doi.gov/files/uploads/tic_ref_arch_v2-0_2013.pdf) "	Version 2.0, October 1, 2013*Version 3 in draft
"Trusted Internet Connections (TIC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf"	OMB M-08-05
"Domain Name System Security(NSSEC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf"	OMB M-08-23
Federal Information Security Modernization Act (FISMA) of 2014	44 U.S.C. § ch.35
Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act of 1996	40 U.S.C
Privacy Act of 1974	5 U.S.C. § 552a
Homeland Security Presidential Directive, “Policy for a Common Identification	HSPD-12
Standard for Federal Employees and Contractors, August 27, 2004	
Management of Federal Information Resources, and Appendix III,	(OMB) Circular A-130
Security of Federal Automated Information Systems”, as amended	OMB Circular A-130
E-Authentication Guidance for Federal Agencies	OMB Memo M-04-04
Standards for Security Categorization of Federal Information and Information Systems	FIPS PUB 199
Minimum Security Requirements for Federal Information and Information Systems	FIPS PUB 200
Security Requirements for Cryptographic Modules	FIPS PUB 140-2
Guide for Developing Security Plans for Federal Information Systems	NIST Special Publication 800-18 Rev 1
Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems	NIST Special Publication 800-30
Contingency Planning Guide for Information Technology Systems	NIST Special Publication 800-34
Guide for the Security Certification and Accreditation of Federal Information Systems	NIST Special Publication 800-37
Security Guide for Interconnecting Information Technology Systems	NIST Special Publication 800-47
Recommended Security Controls for Federal Information Systems	NIST Special Publication 800-53
Guide for Assessing the Security Controls in Federal Information Systems	NIST Special Publication 800-53A
CNSSI 5000	Voice Over Internet Protocol (VoIP) Telephony
CNSSI 5000 ANNEX I	Voice over Secure Internet Protocol (VoSIP)
CNSSI 5000 ANNEX J	Softphone Security Requirements
CNSSI 5001	Type-Acceptance Program for Voice Over Internet Protocol (VoIP) Telephones
CNSSI 5002	Telephony Isolation Used for Unified Communications Implementations Within Physically Protected Spaces
CNSSI 5006	National Instruction for Approved Telephone Equipment
CNSSI 5007	Telephone and Security Equipment Submission and Evaluation Procedures
CNSSI 4005	Safeguarding Communications Security (COMSEC) Facilities and Materials
OMB Memo M19-17	Enabling Mission Delivery through Improved Identity, Credential, and Access Management
OMB Memo M16-04	Cybersecurity Strategy and implementation Plan (CSIP)
E.O 13800	Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
E.O. 13587	Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
CNSSI 1300	Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Under CNSS Policy No. 25

The contractor is responsible for remaining abreast of all new mandatory cybersecurity requirements at both the federal and DOS level and complying with the requirements at the task order level as the requirements are relevant to that task order.

As FAR clauses are published as a result of the May 12th EO on Cybersecurity they will be incorporated into the master IDIQ and apply at the task order level.

In addition to being able to perform in accordance to the referenced publications as required at the Task level for sensitive data and information technology (IT) resources, a contractor must ensure that the contractor's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency ("Federal Information"), which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to the requirements commercial standards that provide a substantially equivalent or greater level of security.

C.1.5 Innovation and Technological Change

The Evolve IDIQ is intended to support all integrated IT services-based solutions, including all current leading-edge technologies and any new technologies, which may emerge during the period of performance. **All IT development methodologies, including Agile which is an encouraged methodology, are supported**. Evolve is intended to provide IT solutions through performance of a broad range of services, which may include the integration of various technologies critical to the services being acquired.

C.2 Five Pools

The Contractor shall furnish the full range of solutions and services necessary to meet requirements of this contract and individual TOs as related to the pools described below. All solutions and services must meet DOS policies, standards, and procedures as identified by individual TOs (e.g. enterprise architecture, information assurance, and personnel, physical and system security).

C.2.1 Pool 1 – IT Management

Summary of Pool 1 - IT Management
Pool 1 consists of the overall management, strategy, and planning of enterprise IT. This includes:

- Enterprise Architecture planning resources for specifying and managing business, information, application, and technical architecture to drive standardization, integration, and efficiency among business technology solutions.
- IT Finance resources involved in the planning, budgeting, spend management and chargeback of IT expenditures and the costing of IT products and services.

- Business solution consulting to help the enterprise improve service delivery through analysis of existing business problems and development of plans for improvement.

Additional services supported under Pool 1 include:

- Technology Business Management, Innovation and Ideation, allowing technology leaders and business leaders to collaborate on solutions for improving business outcomes.
- Resources involved in supporting IT governance, data analytics, IT finance and costing, IT billing, business value, metrics, benchmarking, service portfolio management, service catalog management, service level management and availability management, and performance monitoring and reporting of delivered services performed in Pools 2-5.
- Support for security and compliance to ensure the integrity, protection and proper use of the enterprises technology systems and data. Sets policy, business processes, and establishes controls for Identity & Access Management, Cyber Security & Incident Response, Threat & Vulnerability Management, Data Privacy & Security, Governance, Risk & Compliance, and Business Continuity & Disaster Recovery.

C.2.1 Pool 1 Capabilities

The scope of Pool 1 is listed below, but not limited the following:

Pool 1: IT Management	
Capability Areas within Pool	**Objectives**
1.1: PMO Support	Provide input and support for programmatic activities related to contract tasks.
1.2: Strategic Communications and Engagement	Manage the program's strategic communications and engagement activities, including development of supporting artifacts.
1.3: Strategic Planning	Conduct long term visioning and planning for the direction of IRM and DOS IT systems
1.4: Performance Management	Monitor and report on the contractor's performance to meet mutually agreed upon measures and targets.
1.5: Program Management	Manage the IDIQ contract and tasks orders.
1.6: Transition Management	Facilitate and manage contractor transitions to ensure continuity of support and to maintain system availability, reliability, and customer satisfaction performance standards.
1.7: Enterprise Architecture	Develop business, information, application and technical architecture strategies and roadmaps to drive standardization, integration, modernization, security, and efficiency among business technology solutions.

1.8: Cyber Security & Incident Response	Provide policies, procedures, and technologies to recognize existing and emerging threats as well as determine associated risk to ensure the organization has the appropriate defense and responses to each incident.
1.9: Finance and Budget	Provide planning, budgeting, spend management, chargeback, tracking, reporting, and auditing of IT expenditures and the costing of IT products and services. May include chargeback of IT expenditures and the costing of IT products and services.
1.10: Governance, Risk, Audit, and Compliance	Provide strategy, policies, and processes for managing an overall governance, enterprise risk management and compliance with regulations, with regards to IT. Provides structured approach for aligning IT with business goals and objectives, while managing risk and meeting compliance requirements.
1.11: Process Improvement Consulting	Provide process improvement consulting services with a roadmap to improve efficiency, strengthen system driven management controls, improve security, modernize systems, improve processes or develop them where they don't exist, and reduce cost.
1.12: Zero Trust Architecture	Develop technological roadmaps, plans, and strategies to secure the global network and its resources. This includes strategies for least privilege access, micro-segmentations, data usage controls, continuous monitoring, auditing, etc.
1.13: Executive Support Program	Provide executive coordination and processing, planning, communication in an efficient and streamlined manner.

C.2.1 Cross Functional Responsibilities

The following table summarizes the Cross Tower / Cross Functional categories that all contractors are required to support.

Requirements Category	Description
Compliance	IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.
Security	IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.
Disaster Recovery	IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR

	designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.).
Client Management	Resources or "account managers" aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.
IT Service Management	Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk).
Product and Project Management	Resources involved with managing and supporting IT related projects and/or continuous product development (e.g. Agile) across business and IT-driven initiatives.
Innovation, Ideation, and Modernization	The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services. Includes enterprise architecture solutions that enhance and modernize DOS services.

C.2.1 Non-Exhaustive Sample of Work

A sample, non-exhaustive, sampling of work to be performed under this task area is Listed below.

- Support IT Strategic Planning
- IT Governance Development and Management
- Analytics (Artificial Intelligence and Machine Learning, Data Warehousing, Data
- Mining and Business Intelligence)
- Business Consulting, Business Process Reengineering, and Advisory & Assistance
- Services
- Organizational Management (Change Management, Communications, Balanced
- Scorecard and A-76 Support)
- IT Acquisition Management (Market Research and Analysis and Acquisition Support)
- Program/Project Management Support (Agile Project Management, Agile Coaching,
- Risk Management, Financial Management and Workforce Management)
- Program Management Office Support (IT Portfolio Analysis, Capital Planning and
- Investment Control)
- Program Analyses and Implementation (Business Cases Analysis, Cost/Benefit
- Analysis and Cost Effectiveness Analyses)
- Independent Verification and Validation
- Enterprise Architecture Support
- Program Measurement (Benchmarking, Common Baseline and Gap Analysis)

Pool One IT Security Requirement

Development and implementation of management, operational, and technical security controls required by DOS to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.2.2 Pool 2 – Network Services

Summary of Pool 2 - Network Services

Pool 2 provides the voice and data network and supporting services such as load balancing, domain services, virtual private network, and the internet to enable communications within and outside the enterprise. This Pool includes

- Domain Services, Virtual Private Networks, and Telecommunications using the public internet to enable communications across the organization including its data centers, office buildings, remote locations, partners, and service providers.
- Optimization of incoming application/workload requests through load balancing and traffic management to deliver high availability and network performance to applications.
- Data, voice, and virtual private networks - terrestrial and non-terrestrial (e.g., satellite) technologies as well as field networks or special-use networks.
- Resources to provide physical and wireless local area network connecting equipment within the core data centers and connecting end users in office working areas to the organization's broader networks.

C.2.1 Pool 2 Capabilities

The scope of Pool 2 is listed below, but not limited the following:

Pool 2: Network and Telecom	
2.1: Systems Design and Management	Manage all activities necessary to support the agile design, development, testing, and release new features and capabilities. Includes the patching and security of network and SOE systems.
2.2: Domain Services	Provide lookup capabilities to convert domain names into the associated IP address to enable communication between hosts. Includes Active Directory services and the associated tools required to administer domains.
2.3: Data and Voice Networks	Design, operate, maintain, and modernize network connections that enable direct data and voice communications across the organization including its data centers, office buildings, remote locations as well as partners and service providers (including public cloud service providers). Includes the data network circuits and associated access facilities and

Pool 2: Network and Telecom	
	services; includes dedicated and virtual data networks and internet access. Telephony and wireless.
2.4: Radio Network Installation & Maintenance:	Provide research, development, procurement, design, logistics, installation, and maintenance expertise with HF, UHF, VHF, and satellite radio systems, to include land/mobile radios, handhelds, base stations, vehicle-based, remote, repeaters, and associated encryption capabilities for all. Voice and data network connectivity expenses including circuit and usage expenditures; lease expenditures; maintenance and support expenditures.
2.5: Telecommunications	Engineer, install, configure, provide operational support, and provide turnkey integrated solutions supporting multi-vendor OEM telecommunications platforms.
2.6: Tactical Operations and Field Support	Strategically positioned regional command operations (RIMCs) provide the initial point of contact in support of all overseas communication platforms that fall under the IRM umbrella of control. The availability to quickly leverage additional subject matter experts (personnel) and surge capacity (teams and equipment) for IRM field support is essential for mission success.
2.7: Structured Cabling	Voice and data structured cabling installation, termination, and testing services, to include CAT-X, fiber, coaxial, direct burial, aerial, and associated technologies to support voice and data networks, radio and security systems.
2.8: Operations Center	Centralized IT Operations Center resources including monitoring and intervention e.g., NOC (network operations center), GOC (global operations center).
2.9: LAN/WAN Services	Operate, maintain, and administer physical and wireless local area network connecting equipment within the core data centers and connecting end users in office working areas to the organization's broader networks.

C.2.1 Cross Functional Responsibilities

The following table summarizes the Cross Tower / Cross Functional categories that all contractors are required to support.

Requirements Category	**Description**

Compliance	IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.
Security	IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.
Disaster Recovery	IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.).
Client Management	Resources or "account managers" aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.
IT Service Management	Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk).
Product and Project Management	Resources involved with managing and supporting IT related projects and/or continuous product development (e.g. Agile) across business and IT-driven initiatives.
Innovation, Ideation, and Modernization	The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services. Includes enterprise architecture solutions that enhance and modernize DOS services.

C.2.1 Non-Exhaustive Sample of Work

A sample, non-exhaustive, sampling of work to be performed under this task area is Listed below.

- Network strategy for the global operation
- Data and Voice Network design
- Configuration and installation of network devices
- Management of network devices including configuration, patching, monitoring
- Design and installation of Radio Networks
- Implementation of Telecommunications systems
- Monitoring and reporting of network performance
- Provide field support for network infrastructure
- Installation of cabling at new office locations

Pool 2 IT Security Requirement

Development and implementation of management, operational, and technical security controls required by DOS to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.2.3 Pool 3 – Cloud and Data Services

Summary of Pool 3 – Cloud and Data Services

Pool 3 provides internal and/or external cloud services including IaaS, PaaS, and SaaS. The pool includes:

- Provision a secure and controlled environment for housing compute, storage, network and other technology equipment.
- Licensing, maintenance and support costs for all software including operating system, middleware, databases, system management and administration tools, desktop applications and utilities and business applications. Software costs include enterprise or per instance licenses, client-access licenses, maintenance/update costs, customization fees.
- Resources related to managing the data center environment
- Support for purpose-built facilities to securely house computer equipment: racks/cabinets & cabling, clean & redundant power, data connectivity, environmental controls including temperature, humidity and fire suppression, physical security, and the resources to run and operate the facility and its infrastructure.
- Tools and resources for managing the lifecycles of containers such as the control and automation of tasks such as provisioning and deployment of containers, maintaining availability, scaling up or removing containers to manage application loads, relocating containers, allocating resources for containers, and monitoring container and host health.

C.2.1 Pool 3 Capabilities

The scope of Pool 3 is listed below, but not limited the following:

Pool 3: Cloud and Data Centers	
3.1: Enterprise Data Management	Manage a comprehensive data management program that maximizes the availability and accessibility of high-quality data for consumption by a diverse set of stakeholders.
3.2: Data Access and Integration Program Management	Provide a central point of contact to manage offline relationships with external entities seeking to integrate with the program's technical products and data or that the program requires integration with.
3.3: Virtual Compute and Containers	Provide a variety of compute configurations delivered through the virtualization of physical compute resources. May include on-

	demand provisioning and de-provisioning based on user interaction or the performance of the application itself.
3.4: Technology Lifecycle Management	Ensure that appropriate technologies and their licenses, including new and emerging technologies, can be identified, assessed, acquired, and maintained.
3.5: Cloud Services	Provide and administer cloud solutions such as infrastructure, platform, or software hosted by secure third-party providers and made available to users on demand.

C.2.1 Cross Functional Responsibilities

The following table summarizes the Cross Tower / Cross Functional categories that all contractors are required to support.

Requirements Category	Description
Compliance	IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.
Security	IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.
Disaster Recovery	IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.).
Client Management	Resources or "account managers" aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.
IT Service Management	Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk).
Product and Project Management	Resources involved with managing and supporting IT related projects and/or continuous product development (e.g. Agile) across business and IT-driven initiatives.
Innovation, Ideation, and Modernization	The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services. Includes enterprise architecture solutions that enhance and modernize DOS services.

C.2.1 Non-Exhaustive Sample of Work

A sample, non-exhaustive, sampling of work to be performed under this task area is Listed below.

- 21st Century Integrated Digital Experience Act (IDEA) compliance support
- Managed IT Services Support (e.g., Software-as-a-Service, Platform-as-a-Service,
- Cloud Services, etc.)
- Web Development and Support
- Electronic Commerce and Electronic Data Interchange
- Government to Citizen Relationship Management
- Knowledge Management (IT-based sharing/storing of an Agency individuals'
- knowledge)
- IT–Enhanced Public Relations
- Business-to-Government (B2G) Solutions
- Communications Management
- Accessibility Services (508 and 504 compliance)
- Automated Abstraction, Taxonomies and Ontologies
- Social Media and Social Media Management and Analytics
- Interactive Marketing
- Robotic Process Automation (RPA)

Pool 3 IT Security Requirement

Development and implementation of management, operational, and technical security controls required by DOS to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.2.4 Pool 4 – Application Development

Summary of Pool 4 – Application Development

Pool 4 provides software application development, testing, release, support, and operations. This Pool includes:

- Resources involved with the analysis, design, development, code, test, and release packaging services associated with application development projects.
- Operations, support, fix, and minor enhancements associated with existing applications.
- Distributed and mainframe databases, middleware systems and DBMS software and tools support.
- Distributed database services focused on the physical database (versus the logical design) including DBAs, DBMS, tools, and operational support
- Distributed platform, application and system integration resources enabling cross application development, communications, and information sharing
- Mainframe database services focused on the physical database (versus the logical design)

- Mainframe platform, application and system integration resources enabling cross application development, communications, and information sharing.

The Contractor shall provide all phases of software design and development including deployment to ensure DOS applications and databases will enable their users to meet their mission goals and objectives. These efforts include the full range of software design, development, implementation and integration, including, but not limited to, concept development, planning, requirements definition and analysis, systems design and development, coding and testing, production, deployment, implementation, integration, and software application maintenance.

Application Services provide support for all applications and collaborative service capabilities. These services include support for developing and implementing enterprise and departmental-level applications. These applications may have inter-related service processing components extending across/beyond the enterprise, or unique to a particular mission's requirements

The Contractor shall promote, to the maximum extent practicable, use of commercially available technologies (e.g. Commercial Off-the-Shelf (COTS) and non-developmental items) to support Federal government agencies' IT solution requirements. The Contractor shall provide competencies to employ DOS enterprise architectures (EAs) as required by individual Orders.

The Contractor shall provide Applications Services for systems required to support unique agency and departmental-level mission requirements, as specified in individual Orders. These services include support for existing and/or new/emerging mission requirements.

C.2.1 Pool 4 Capabilities

The scope of Pool 4 is listed below, but not limited the following:

Pool 4: Application Development	
4.1: System Management and Configuration Changes	Manage the technical system, including sub-components and supporting technologies, to ensure overall system reliability, flexibility, and availability with minimal disruptions to service.
4.2: Security and Contingency Planning, Preparation, and Operations	Develop, maintain, and test appropriate security and contingency plans to comply with relevant policies, directives, and industry best practices for securing developed applications.
4.3: User Experience Deign	Manage and conduct all activities necessary to identify customer and user requirements and design solutions using a human-centered design approach.
4.4: Development	Manage prioritization of requirements across the system, and continuously manage and perform the necessary development activities using an agile and integrated approach that maximizes proposed productivity measures.
4.5: Testing	Develop, conduct, integrate and manage all testing needed to ensure production-ready development.

4.6: Release Management	Manage the technical release of features throughout the development lifecycle.
4.7: Database, Mainframe, Middleware	Operate and maintain distributed and mainframe databases and middleware systems as well as include DBMS software and tools.

C.2.1 Cross Functional Responsibilities

The following table summarizes the Cross Tower / Cross Functional categories that all contractors are required to support.

Requirements Category	Description
Compliance	IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.
Security	IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.
Disaster Recovery	IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.).
Client Management	Resources or "account managers" aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.
IT Service Management	Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk).
Product and Project Management	Resources involved with managing and supporting IT related projects and/or continuous product development (e.g. Agile) across business and IT-driven initiatives.
Innovation, Ideation, and Modernization	The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services. Includes enterprise architecture solutions that enhance and modernize DOS services.

C.2.1 Non-Exhaustive Sample of Work

A sample, non-exhaustive, sampling of work to be performed under this task area is listed below.

- Requirements Analysis/Gathering, Design, Coding, Security and Testing
- Artificial Intelligence (Software and Services)
- Secure Code Management
- Production Deployment
- Application Prototyping
- Multimedia Software for Patient/Staff Education
- Program Evaluation Software
- Administrative and General Decision Support Software
- Web X.0 (2.0, 3.0, …) Development and Management
- Database Development and Management
- Clinical Protocol and Quality Assurance Decision Support Software
- Testing
- Enterprise Software planning and implementation

Pool 4 IT Security Requirement

Development and implementation of management, operational, and technical security controls required by DOS to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

C.2.5 Pool 5 – End User Services

Summary of Pool 5 – End User Services

Pool 5 provides end user computing devices and support for end users. This Pool includes:

- Costs to build, manage and run end user computing devices for the enterprise and deliver centralized support to end users
- Support for client compute physical desktops, portable laptops, thin client machines, peripherals (including monitors, pointer devices and attached personal printers) used by individuals to perform work.
- Support for mobile devices such as client compute tablets, smart phones (iOS, Android, Windows Mobile) and apps used by individuals to perform work. I
- Support for client related software used to author, create, collaborate, and share documents and other content.
    - Examples include email, communications, messaging, word processing, spreadsheets, presentations, desktop publishing, and graphics
- Support for network printers, audio and video conferencing equipment typically used in conference rooms and dedicated telepresence rooms to enable workforce communications

- Centralized Tier 1 help desk resources that handle user requests, answer questions, and resolve issues, and local support resources that provide on-site support for moves, adds, changes and hands-on issue resolution.

C.2.1 Pool 5 Capabilities

The scope of Pool 5 is listed below, but not limited the following:

Pool 5: End User and Customer Support	
5.1: Help/Support Desk	Provide 24/7 Tier 0, 1 and 2 customer and technical support using multiple support channels (e.g., chatbots, voice, in app, etc.), maximizing the use of automation.
5.2: Change Management &User Communications	Provide and facilitate multi-channel communications with users about upcoming events, available resources, and changes to the user interface and related business processes, best practices, and process improvement recommendations
5.3: Training	Develop, maintain, and deliver comprehensive multi-modal instructional systems training of DOS systems and applications.
5.4: Technical Security Services	Safeguard, Protect, apply countermeasures to classified Information Communications equipment(ICT) deployed at US embassies and domestically. TEMPEST.
5.5: Mobile and Remote Access	Provide mobile and remote access for services such as GO Browser, GO Virtual, mobile device management and support, and other mobile services.

C.2.1 Cross Functional Responsibilities

The following table summarizes the Cross Tower / Cross Functional categories that all contractors are required to support.

Requirements Category	**Description**
Compliance	IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.
Security	IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cyber Security & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.
Disaster Recovery	IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR

	designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.).
Client Management	Resources or "account managers" aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.
IT Service Management	Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk).
Product and Project Management	Resources involved with managing and supporting IT related projects and/or continuous product development (e.g. Agile) across business and IT-driven initiatives.
Innovation, Ideation, and Modernization	The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services. Includes enterprise architecture solutions that enhance and modernize DOS services.

C.2.1 Non-Exhaustive Sample of Work

A sample, non-exhaustive, sampling of work to be performed under this task area is Listed below.

- Manage Service Desk for Level 0,1,2 and dispatch
- Implement automation in Service Desk and End-User support
- Management and distribution of images for end-user devices
- Develop training materials for DOS applications
- Set up training facilities at DOS locations
- Support video conferencing for global meetings

Pool 5 IT Security Requirement

Development and implementation of management, operational, and technical security controls required by DOS to assure desired levels of protection for IT systems and data are achieved (e.g., establishment of policy/procedures in support of Federal IT security requirements, conduct risk assessments to identify threats/vulnerabilities for existing/planned systems; support Federal mandates for measuring and reporting compliance, perform certification and accreditation (C&A) activities; provide training services to promote awareness and knowledge of compliance responsibilities for Federal IT security requirements).

(End of Section C)

SECTION D - PACKAGING AND MARKING

D.1 Packing, Packaging, Marking and Storage of Equipment

Unless otherwise specified, all items to be delivered under this contract shall be preserved, packaged, and packed in accordance with normal commercial practices to meet the packing requirements of the carrier and ensure safe delivery at destination.

All initial packing, marking and storage incidental to shipping of equipment to be provided under this contract shall be at the Contractor's expense. The Contractor shall supervise the packing of all acquired equipment furnished by the Contractor and shall supervise the unpacking of equipment to be installed.

D.2 Markings

All deliverables submitted to the Contracting Officer, the Evolve Program Manager, the TO Contracting Officer or the TO COR shall be accompanied by a packing list or other suitable shipping document that shall clearly indicate the following:

(a) Contract number;
(b) Task order number;
(c) Name and address of the consignor;
(d) Name and address of the consignee;
(e) Government bill of lading number covering the shipment (if any); and
(f) Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).

Specific marking requirements may be addressed in individual TOs.

D.3 Equipment Removal

All Contractor-owned equipment, accessories, and devices located on Government property shall be dismantled and removed from Government premises by the Contractor, at the Contractor's expense, within 60 calendar days after contract expiration, or as mutually agreed by the Government and the Contractor. Exceptions to this requirement shall be mutually agreed upon and written notice issued by the TO Contracting Officer. Specific requirements will be addressed in individual TOs.

(End of Section D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1 Clauses Incorporated by Reference- TBD

E.2 Inspection and Acceptance

(a) Inspection and acceptance of all work and services performed under each TO will be in accordance with the FAR clauses incorporated at Section E, *Clauses Incorporated by Reference* as applicable.

(b) Final acceptance of all deliverables and or services performed as specified under each Task Order will be made in writing, at destination by the TO COR or as detailed in individual TOs.

E.3 Scope of Inspection

(a) All deliverables will be inspected for content, completeness, and accuracy and conformance to task order requirements by the TO COR or as detailed in individual task orders. Inspection may include validation of information or software through the use of automated tools and/or testing of the deliverables, as specified in the task order. The scope and nature of this testing must be negotiated prior to TO award and will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

(b) The government requires a period not to exceed thirty (30) calendar days after receipt of final deliverable items for inspection and acceptance or rejection unless otherwise specified in the TO.

E.4 Basis of Acceptance

(a) The basis for acceptance shall be compliance with the requirements set forth in the statement of work, the TO, the Contractor's proposal and other terms and conditions of this contract. Deliverable items rejected under any resulting task order shall be corrected in accordance with the applicable clauses.

(b) Commercial and non-developmental hardware items, software items, pre-packaged solutions, and maintenance and support solutions will be accepted within thirty (30) calendar days of delivery when performance is in accordance with delivery requirements.

(c) Custom services and cost reimbursable items such as travel and ODCs will be accepted upon receipt of proper documentation as specified in the order. If custom services are provided as part of a FFP TO, acceptance will be as specified for the milestone with which they are associated. If custom services are for software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the government have been resolved, either through documentation updates, program correction, or other mutually agreeable methods.

(d) Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the government have been corrected.

(e) Non-conforming products or services will be rejected. Unless otherwise agreed by the parties, deficiencies will be corrected within 30 calendar days of the rejection notice. If the deficiencies cannot be corrected within 30 days, the Contractor will immediately notify the TO Contracting Officer of the reason for the delay and provide a proposed corrective action plan within 10 working days.

E.5 Review of Deliverables

(a) The government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) business days from receipt by the Government of the initial deliverable.

(b) Upon receipt of the Government comments, the Contractor shall have fifteen (15) business days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form.

(c) If written acceptance, comments and/or change requests are not issued by the Government within 30 calendar days of submission, the draft deliverable shall be deemed acceptable as written and the Contractor may proceed with the submission of the final deliverable product.

E.6 Written Acceptance/Rejection by the Government

The Government shall provide written notification of acceptance or rejection of all final deliverables within 30 calendar days. Absent written notification, final deliverables will be construed as accepted. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

(End of Section E)

SECTION F - DELIVERIES OR PERFORMANCE

F.1 Clauses Incorporated by Reference- TBD

F.2 Term of the Contract

The term of this indefinite delivery indefinite quantity (IDIQ) contract is a base five year period. This is not a multi-year contract as defined in FAR Part 17.1.

F.3 Task Orders Performance Period and Pricing

Task Orders (TOs) may be issued at any time during the base period and/or option periods. The performance period will be specified in the TO and may include option periods which extend the TO up to sixty (60) months beyond the expiration date of this contract. TOs shall be priced using the Section B rates that will be applicable to the TO's anticipated period of performance.

For purposes of TOs that extend beyond the expiration date of the contract, the final contract year's pricing shall be used. However, Task Order Contracting Officers may negotiate rate escalations for periods beyond the contract expiration.

F.4 Option To Extend Term Of Contract (FAR 52.217-9) (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor at any time within the term of the contract, provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least thirty (30) days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

F.5 Delivery

The items required under each individual TO shall be delivered and received at destination within the timeframe specific in each order.

F.6 Place of Performance

Place of performance shall be set forth in individual TOs.

F.7 Notice to the Government of Delays

In the event the Contractor encounters difficulty in meeting performance requirements, or when he anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the TO Contracting Officer and the TO COR, in writing, giving pertinent details; provided,

however, that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

F.8 Deliverables

(a) All applicable deliverables, their required delivery dates, and destination of delivery will be specified in each task order issued under this contract. The schedule for completion of work to be performed under this contract will be delineated in each TO issued under this contract, as applicable.

(b) For purposes of delivery, all deliverables shall be made by close of business (COB) 4:30 P.M. local time (Washington, DC) at destination, Monday through Friday, unless stated otherwise in the TO.

(c) All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

(d) Each contract-level and TO-level deliverable shall be accompanied by a cover letter from the Contractor on Company letterhead. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.

(e) In the event the Contractor anticipates difficulty in complying with any contract-level delivery schedule, the Contractor shall immediately provide written notice to the Contracting Officer and the Evolve Program Manager. For any task order level deliverable, the Contractor shall provide written notification immediately to the task order-level Contracting Officer and TO COR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; PROVIDED, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.

F.9 Contract Status Report

The Prime Contractor shall provide a monthly task order activity report, organized by DOS Component, to the Contracting Officer and the EVOLVE Program Manager. The sample format is provided in Attachment J-1, *Sample Monthly Contract Status Report*. The report is due by the 15th calendar day of each month with a copy to the Contracting Officer and the EVOLVE Program Manager. Additionally, the Contractor shall provide copies of all task orders, including task order modifications, to the Evolve Program Manager.

F.10 Annual Program Management Plan

The Prime Contractor shall provide a Program Management Plan (PMP) that gives a description and graphic summary of the schedule and financial components of the task/delivery order. The PMP shall be based on the Contractor's Work Breakdown Structure (CWBS) (Attachment TBD) as well as technical direction for the coming year and summary schedules for

succeeding fiscal years. Staffing levels for the prime contractor and subcontractors shall be identified to the nearest 0.1 person along with the rationale used in computing the staffing levels.

F.11 Monthly Program Status Report

The Prime Contractor shall provide a Program Status Report (PSR) that documents the progress of the contractual effort as of the report date. The PSR shall describe any area of difficulty and the contractor's approach to resolving them while maintaining baseline plans. The PSR shall apprise DOS of the contractor's assessment of each project's performance to date in relation to a Master Milestone Schedule and cost/schedule performance baseline. A funding status report shall be included in this deliverable. Action items for both the contractor and DoS shall be included along with appropriate graphs, charts, and illustrations.

F.12 Monthly Cost Performance Report

The Prime Contractor shall provide a Cost Performance Report (CPR) that provides State management with costs incurred and progress against the previous monthly schedule. These costs shall be keyed to the CWBS. The report shall include cumulative data from contract inception through the report month. The report shall include the actual and invoiced costs. The data shall be reported in accordance with the standards indicated in the task/delivery order showing earned value and variances. A CWBS increment of work (e.g., the task area level) shall be considered out-of-tolerance if the year-to-date actuals exceed the budgeted amount by 2 percent or more. A variance analysis shall be provided as explanation for out-of-tolerance variances.

F.13 Monthly Master Milestone Schedule

The Prime Contractor shall provide a monthly Master Milestone Schedule (MMS) that shall contain projected and actual schedules versus progress with technical direction deliverables and other milestones clearly identified. Approved modification of baseline schedules shall be clearly delineated from the original baseline.

F.14 Monthly Performance Summary Report

The Prime contractor shall provide a Performance Summary Report that summarizes contractor performance for the designated reporting period.

F.15 Monthly Procurement Reports

The Prime Contractor shall submit monthly invoices that contain supporting documentation for purchases and expenses, such as travel receipts, materials costs, and/or any other supporting documentation requested by the Government. The Government will not require supporting documentation that is contrary to the contractor's DCAA approved accounting system (if applicable).

F.16 Monthly Labor Reports

The Prime Contractor shall provide monthly reports that provide detailed accrual and invoiced costs for labor (actual and cumulative). The reports shall include charts that demonstrate cumulative spending. The contractor's Program Manager shall ensure the accuracy of all hours entered into a DOS time tracking system, as required and when available.

F.17 Task Order Status Reports

Evolve requires TO Status Reports for all TOs. The type of status report may vary by the type of TO issued. The status report recipients, content, and due dates will be identified in individual TO Request for Proposal. The TO Status Report shall be at the task order level unless a lower Work Breakdown Structure (WBS) level of reporting is explicitly required and stated in the TO Request for Proposal.

F.18 Subcontracting Plan Reports- TBD

F.19 Comprehensive Contracts Report

Within 30 calendar days after contract award, the Contractor shall submit a comprehensive and accurate report listing of all active contracts/task orders it currently has within DOS and its Components that fall within the scope of the Evolve contract. The report shall include, at a minimum, the following information for each contract/order:

(a) Contract/order number;
(b) Brief Description of the work being performed;
(c) Issuing office name and address;
(d) Contact information for the issuing Contracting Officer;
(e) Contact information for the associated COR(if any);
(f) Overall dollar value; and
(g) Period of performance, including base and option periods.

The report shall be submitted to the address identified in Section G.2. Accuracy and timeliness of this deliverable are considered critical to the implementation of the Evolve program and failure to comply may adversely affect the Contractor's ability to participate in TO competitions.

F.20 Annual Supply Chain Risk Management (SCRM) Plan Submission

To ensure Contractors remain aware of and are implementing emerging SCRM requirements over the life of the Master Contract, a SCRM Plan will be submitted to the Program Manager no later than 30 calendar days after the end of each contract year. Refer to NIST SP 800-161 for a plan template.

(End of Section F)

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 Accounting and Appropriation Data

Accounting and appropriation data for obligations under the contract will be set forth on individual task orders (TOs).

G.2 Points of Contact

The following subsections describe the roles and responsibility of individuals who will be the primary points of contact for the Government on matters regarding contract administration as well as other administrative information. The Government reserves the right to unilaterally change any of these individual assignments at anytime.

Evolve Program Manager:
Name: Kimberly Baltimore
Email: BaltimoreKD@state.gov

Task Order Manager: To be provided for each order where applicable

E-mail communications shall make reference to the contract number and shall be e-mailed to BaltimoreKD@state.gov.

G.2.1 Contracting Officer (CO) – Contract Level

(a) The Contracting Officer (CO) has the overall responsibility for the administration of this contract. The CO, without right of delegation, is the only authorized individual to take actions on behalf of the Government to amend, modify or deviate from the contract terms, conditions, requirements, specifications, details and/or delivery schedules. The CO may delegate certain specific responsibilities to its authorized representative--the Contracting Officer's Representative (COR). The CO may also designate an alternate COR for this contract.

(b) The COR, hereafter referred to as the Evolve Program Manager, for this contract will be identified by the Contracting Officer through a written designation. A copy of the letter of designation with specific duties and responsibilities will be provided to the Contractor.

G.2.2 Task Order Contracting Officer (TO CO)

Services will be ordered via task orders issued by TO COs within the Contract User's organization following the ordering procedures set forth in Section G.4.

G.2.3 Task Order Contracting Officer's Representative (TO COR)

TO COs may designate CORs for individual task orders that will be responsible for the day-to-day coordination of the Task Order.

The TO COR will represent the TO CO in the administration of technical details within the scope of the task order. The TO COR is also responsible for the final inspection and acceptance of all task order deliverables and reports, and such other responsibilities as may be specified in the

task order. The TO COR is not otherwise authorized to make any representations or commitments of any kind on behalf of the TO CO or the Government. The TO COR does not have authority to alter the Contractor's obligations or to change the task order specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify task order obligations or the specification, changes will be issued in writing and signed by the TO CO.

G.2.4 Contractor's Program Manager

The Program Manager shall act as the central point of contact with the Government for all program-wide technical issues and will represent the Contractor at all post-award status meetings. The Program Manager shall be responsible for all issue resolution, program management, and other contract support including providing comprehensive account support for the Evolve contract. The Program Manager is responsible for overall contract performance and shall not serve in any other capacity under this contract.

G.3 Ordering–By Designated Ordering Official

The Government will order any supplies and services to be furnished under this contract by issuing task orders on Optional Form 347, or an agency prescribed form, from the effective date of the contract through the expiration date of the contract.

G.3.1 Direct Ordering

Evolve services shall be ordered by the issuance of task orders in accordance with Section G.4-Task Order Procedures and FAR Part 52.216-18. The Contract Users may directly place orders under the contract to obtain services. The TO CO will be responsible for the issuance, administration, payment and closeout of the order (See also Section G.4). All orders are subject to the terms and conditions of this contract. In the event of conflict between an order and this contract, the contract shall prevail.

In no event will a task order change the requirements of the Evolve contract. Should the Contract User require such a change, specific approval must first be obtained from the CO.

G.3.2 Special Contract Administration Responsibilities

Each Contract User utilizing Evolve has the primary responsibility for the administration of any order it places with the Contractor.

The TO CO shall be responsible for:

(a) Ensuring that task orders are within the scope of the contract;
(b) Administering and final closeout of task orders;
(c) Performing inspection and acceptance or rejection of the equipment/services provided by the Contractor;
(d) Making payment, withholds, or partial payment of Contract User invoices; and
(e) Forwarding end of fiscal year notification to the Contracting Officer; either by (memo, letter, or electronically) that all Contract User task orders awarded in preceding fiscal year are closed and final disposition complete including release of claims letters (if applicable);

The Contracting Officer is responsible for overall administration and the final closeout of the contract, and when necessary, shall:

(a) Provide scope oversight;
(b) Serve as liaison between the Contractor and the Department;
(c) Assist in expediting orders;
(d) Ensure compliance with contract requirements;
(e) Issue the Contracting Officer's final decision and handle all contract-level contractual disputes under the Contract Disputes Act; and
(f) Place all contract modifications against the Contract.

Unless otherwise delegated, only the designated CO, as defined in Section G.2, has oversight of the contract as a whole.

G.4 Task Order (TO) Procedures

The Contractor's IT services shall be obtained on an as-needed basis (i.e., through the issuance of task orders). The Contractor shall perform the required effort for these services, both within and outside the United States, throughout the term of this contract. An individual TO may relate to a single Pool or involve services from multiple Pools. Issued TOs will identify the IT services required, provide specific technical details (including the schedule for all deliverables and the identification of any applicable Government-Furnished Property (GFP), Government-Furnished Information (GFI) and/or Government furnished workspace) and activate performance.

The following defines the process by which fair opportunity will be afforded, how a TO will be processed, priced, and awarded. It also defines specific, local provisions to be used for issues concerning task order consideration and payment. Finally, the role of the DOS Ombudsman is defined. Careful attention should be paid to those areas in which the procedures, processes and provisions change due to use of a different contract types or pricing methodology.

G.4.1 Fair Opportunity Process

A GFMS system generated TO tracking number will be assigned to each task order requirement. Unless one of the exceptions at FAR Part 16.505(b)(2) applies, the TO CO will post each task order requirement via e-mail and solicit responses in accordance with Section G.4.3. This announcement satisfies the requirement for a fair opportunity to be considered. Each Contractor shall evaluate the opportunity and determine whether or not to submit a proposal. The announcement will include, at a minimum, the following information:

(a) TO Tracking Number;
(b) Date of Announcement;
(c) End User DOS Office;
(d) Statement of Objectives (SOO) or Statement of Work (SOW) or Performance Work Statement (PWS);
(e) Anticipated Contract Type;
(f) Incumbent Contractor, if any;
(g) Contracting Agency POC Name Phone Number (CO and Contract Specialist); and
(h) E-mail Address and Proposal Due Date.

G.4.2 Fair Opportunity Exceptions.

In accordance with the Federal Acquisition Streamlining Act (FASA) and FAR Part 16.505(b), the TO CO will provide all awardees a "fair opportunity" to be considered for each order in excess of SAT, unless one of the conditions, below, applies.

(1) The agency need for such services is so urgent that providing a fair opportunity would result in unacceptable delays.
(2) Only one awardee is capable of providing the services required at the level of quality required because the services ordered are unique or highly specialized.
(3) The order must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to a task order already issued under this contract, provided that all awardees were given a fair opportunity to be considered for the original order.
(4) It is necessary to place an order to satisfy a minimum guarantee.

In accordance with FAR Part 16.5, when an exception to the fair opportunity to be considered exists, the task order will be processed as a sole source procurement, including a sole source justification.

G.4.3 Task Order Solicitation

Each Task Order will identify the Pool of the work to be performed. For services that cross multiple Pools, the Government will identify the predominant Pool and each Prime Contractor in that Pool will be given the fair opportunity to compete.

G.4.4 Task Order Process

(a) The Contract User will submit a complete Task Order Request Package (TORP) to the TO CO. The package should include an approved purchase request, either a statement of objectives (SOO), statement of work (SOW), or a performance work statement (PWS), and an Independent Government Cost Estimate (IGCE). Performance-based work statements must be used to the maximum extent practicable. Individual TOs must clearly describe all services to be performed or supplies to be delivered. Also, the proposal request will include price/cost and past performance as evaluation factors.

(b) The TO CO will issue a proposal request to all Contractors, unless a fair opportunity exception applies, or the task is set-aside for the small business Prime Contractors. The proposal request will include a due date for proposal submission and either a SOO, SOW or PWS, that will include either the Government's objectives or a detailed description of work to be accomplished, the applicable task areas, a listing of the deliverables required and any additional data, as appropriate. The proposal request will also include specific instructions for the submission of proposals, selection criteria factors, the factors' order of importance and other information deemed appropriate.

(c) Contractors will be provided an adequate time to prepare and submit responses based on the estimated dollar value and complexity of the proposed TO. The due date will be set forth in each proposal request. If unable to perform a requirement, Contractors shall submit a "no bid" reply in

response to the proposal request. All "no bids" shall include a brief statement as to why the Contractor is unable to perform, i.e. conflict of interest.

(d) Technical Proposals. The proposal request will state whether an oral proposal is required in addition to, or instead of, written technical proposals. Responses will be streamlined and succinct, to the extent practical based on the estimated dollar value and complexity of the work, stating compliance or exception to requirements, risks, assumptions, and conflict of interest issues. Responses will not be a proposal as defined in FAR Part 15, but only sufficient information to be considered in accordance with FAR Part 16. Proposals shall not merely restate SOO, SOW or PWS requirements. Both oral and written technical proposals shall address, as a minimum:

(1) Technical/Management Approach;
(2) Key Personnel Assigned;
(3) Quantities/Hours of Personnel by Labor Categories;
(4) Other Direct Costs (ODCs) (materials and supplies, travel, training, etc.);
(5) Risks;
(6) Period of Performance;
(7) Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI);
(8) Security (including clearance level);
(9) Teaming Arrangement (including subcontracting); and
(10) Other Pertinent Data, (e.g., potential conflict of interest issues).

(e) Cost Proposals. TBD

(3) Other Relevant Information. This information shall always be in writing and shall address other relevant information as required by the contract or requested by the TO proposal request. The Contractor shall assume all costs associated with preparation of proposals for task order awards under the fair opportunity process as an indirect charge. The Government will not reimburse awardees for fair opportunity proposals as a direct charge.

(f) Evaluation of TO Proposals. Proposals will be evaluated in accordance with the selection criteria set forth in the TO proposal request. The Government's award decision will be based, at a minimum, on compliance with Section 508 requirements of the Rehabilitation Act, and selection criteria which addresses past performance, technical/ management approach and cost. Among other sources, evaluation of past performance will be based on a database built from past performance assessments provided by TO CORs on individual TOs performed throughout the life of the contract (See Section H.11). In addition to past performance, technical/management approach and cost, individual task order selection criteria may include other factor(s) relevant to the requirement. The order of importance for the factors will be identified in each individual request for proposal. If necessary, during the evaluation of proposals, the Government may contact a Contractor with questions concerning its proposal. Upon completion of evaluations, the CO will issue a task order to the Contractor whose proposal is most advantageous to the Government.

(g) Award Recommendation Documentation. After completion of the evaluation, discussions, if any, and Best Value analysis, the TO CO/TO COR shall prepare a complete award

recommendation package to document the selection process and to serve as evidence that the fair opportunity to be considered rule was applied, unless an exception was taken under FAR Part 16.505(b)(2). At a minimum, it shall include:

(1) A statement indicating whether announcement of the task order requirement was made to all Contractors eligible for receiving an award for the task requirement or if an exception to the fair opportunity to be considered rule was cited (cite the exception);
(2) The selection criteria /methodology used to evaluate the competing Contractors;
(3) The results of the evaluation; and
(4) The rationale for the recommendation of the task order awardee, including a summary of any negotiations conducted, cost/price analysis and best value analysis.

(h) Resolution of Issues. In the event issues pertaining to a proposed task cannot be resolved to the satisfaction of the TO CO, the TO CO reserves the right to withdraw and cancel the proposed task. In such event, the Contractor shall be notified in writing of the TO CO's decision. This decision is final and conclusive and shall not be subject to the "Disputes" clause or the "Contract Disputes Act."

(i) Task Order Issuance. TOs may be issued by e-mail , or an agency prescribed form.

G.4.5 Unauthorized Work

The Contractor is not authorized at any time to commence TO performance prior to issuance of a signed TO or other written approval provided by the TO CO to begin work.

G.4.6 Task Funding Restrictions

No unfunded TOs are allowed.

G.4.7 Changes in Time-and-Materials (T&M) Task Orders

The Contractor shall submit a request for contract modification to the contract level CO to add any new labor categories beyond the Government-required labor categories (See Section G.4.4(e)). Upon contract modification, the Contractor shall submit a revised TO cost proposal to the TO CO showing the original amount of the TO award, the proposed revised amount and the difference.

G.4.8 Debriefings

If a non-selected Contractor has questions as to why it was not selected for a TO award, the Contractor should contact the TO CO. The TO CO and the non-selected Contractor may discuss the reasons why that Contractor was not selected; however, the TO CO may not (1) discuss the other Contractor's proposals, (2) compare Contractor's proposals, or (3) allow the non-selected Contractor access to the award decision documentation.

G.4.9 Task Order Protests

In accordance with FAR Part 16.505(a)(9) no protest under Subpart 33.1 is authorized in connection with the issuance or proposed issuance of a TO under this contract, except for a protest on the grounds that the order increases the scope, period, or maximum value of the contract.

G.4.10 Task/Delivery Order Contract Ombudsman

(a) In accordance with FAR Part 16.505(b)(5), the Task/Delivery Order Contract Ombudsman for this contract is the Director, Office of Acquisition Policy and Oversight within the Office of the DOS Chief Procurement Officer. The Ombudsman responsibilities are to address Contractor concerns regarding compliance with the award procedures for task/delivery orders, review Contractor complaints on task/delivery order contracts, ensure all Contractors are afforded a fair opportunity to be considered for each task/delivery order, consistent with FAR 16.505(b), and when requested, maintain strict confidentiality of the Contractor requesting assistance.

(b) The Ombudsman shall not participate in the evaluation of proposals submitted on the basic contract, the source selection process on the basic contract, or the adjudication of formal contract disputes arising under the basic contract or any individual order issued under it.

(c) Interested parties may contact the Task/Delivery Order Contract Ombudsman by contacting: TBD

G.5 Ordering (Indefinite Delivery Type Contracts)

All Warranted Contracting Officers of the DOS are authorized ordering officers. Supplies or services to be furnished under this contract shall be furnished at such times as ordered by the issuance of Orders on Optional Form (OF) 347 by the CO. All orders are subject to the terms and conditions of the contract. This contract shall control in the event of conflict with any order.

G.5.1 Ordering Procedures

TOs issued shall include, but not be limited to the following information (when applicable):

(a) Date of order;
(b) Contract and order number;
(c) Type of Order;
(d) Appropriation and accounting data;
(e) Description of the services to be performed;
(f) Description of end item(s) to be delivered;
(g) DD Form 254 (Contract Security Classification Specification);
(h) Contract Data Requirements List;
(i) The individual responsible for inspection/acceptance;
(j) Period of performance/delivery date;
(k) Estimated number of labor hours for each applicable labor category;
(l) The estimated cost plus fixed fee or ceiling price for the order; and
(m) List of Government furnished equipment, material, and information.

G.5.2 Modification of Orders

The Cost-Plus Fixed Fee (CPFF) or Ceiling Price for each TO may not be changed except when authorized by a modification to the TO.

G.5.3 Unilateral Orders

TOs under this contract will ordinarily be issued after both parties agree on all terms. If the parties fail to agree, the TO CO may require the Contractor to perform and any disagreement shall be deemed a dispute within the meaning of the "Disputes" clause.

G.6 Preparation of Vouchers-TBD

G.7 Quick-Closeout Procedure

The Contractor is authorized to use the quick-closeout procedure for TOs issued under this contract in accordance with FAR 42.708, Quick-Closeout Procedure.

(a) In accordance with FAR 42.708(a), the TO Contracting Officer has the authority to negotiate settlement of indirect costs for a specific TO if it is physically complete; the amount of unsettled indirect cost to be allocated to the TO is relatively insignificant; and agreement can be reached on a reasonable estimate of allocable dollars.

(b) In accordance with FAR 42.708(b), a determination of final indirect costs under the quick-closeout procedures shall be final for the TO it covers and no adjustment shall be made to other contracts for over- or under-recoveries of costs allocated or allocable to the contract covered by the agreement.

(c) Final invoices which result in a charge to the Government in excess of $250.00 or refunds to the Government in excess of $250.00 shall be processed prior to quick-closeout of the TO.

(d) Submission of a final “0-dollar invoice” is not required. Once agreement for quick-closeout is reached on individual TOs, a bilateral modification will be issued to closeout the TO. Once the bilateral modification is executed by the CO, the TO is closed and no further invoicing, adjustments, or claims will be accepted.

(e) All TOs under this contract do not have to be closed in accordance with quick-closeout procedures. The TO CO and the Contractor will evaluate complex TOs on a case-by-case basis for applicability of quick-closeout procedures.

(f) Modifications for quick-closeout will include the following statement: “The bilateral execution of this modification releases the Government and [insert Contractor name] from any further obligation.”

(End of Section G)

SECTION H – SPECIAL CONTRACTING REQUIREMENTS

H.1 Authorized Users

This Department-Wide Acquisition Contract is available for the use by the Department of State.

H.2 Minimum Dollar Guarantee and Maximum Contract Limitation

(a) Minimums. Each Contractor is guaranteed a total minimum of $250. The minimums are to be obligated during the first year of the base period and are inclusive of fee.

(b) Maximums. The maximum cumulative dollar ceiling value of all contracts in this multiple award procurement is established at $8 Billion.

(c) The Government has no obligation to issue TOs to the Contractor beyond the amount specified in paragraph (a) of this clause. Once the conditions of paragraph (a) have been met, the Contractor will continue to have the opportunity to be issued TO(s) under the Fair Opportunity to Compete provisions in Section G.

(d) Funding will be cited on individual TOs and not on the base contract award.

H.3 Hardware and Software Acquisition

Evolve is a "Solutions Based Contract." The Government anticipates that the majority of work awarded under this contract will be professional services. However, the contract is structured to permit purchase of a full range of electronic and information technology solutions, including hardware, software, bandwidth, and enabling products necessary to implement these solutions. Inclusion of hardware/software/bandwidth acquisition on a TO is within the purview of the cognizant Government CO. Any hardware/software/bandwidth included must be considered to be critical and related to the services being acquired under a TO. Proposals submitted in response to individual TOs shall clearly identify and price any hardware, software or other products included as part of the Contractor's proposal. Unless otherwise indicated, acceptance of a TO proposal resulting in issuance of a TO constitutes authorization to provide the proposed solution, including the hardware, software, bandwidth or other products proposed, subject to the requirements of Section H.5, Contractor Justification for Other Direct Costs (ODCs).

The Government reserves the right to require or otherwise provide preference on Contractor solutions that include specific models of desktop computers, notebooks and monitors qualified through the GITM program or other required programs. Specific requirements will be identified in Task Order Request Packages.

H.4 Purchasing System

The Contractor shall notify the CO in writing if there is any change in the status of its approved purchasing system and provide the reason(s) for the change. Documentation required to be submitted for CO consent shall be submitted in accordance with FAR Part 44, Subcontracting Policies and Procedures.

H.5 Materials-TBD

H.6 Selected Items of Costs

H.6.1 Travel Costs (Including Foreign Travel) TBD

H.6.2 Training

The Government will not allow costs, nor reimburse costs associated with the Contractor training employees to attain and/or maintain minimum personnel qualification requirements of this contract. Other training may be approved on a case-by-case basis by the TO CO. Attendance at workshops or a symposium is considered training for purposes of this clause.

H.6.3 General Purpose Office Equipment (GPOE) and IT

The cost of acquisition of GPOE and IT shall not be allowable as direct charges to this contract. The Contractor is expected to have the necessary facilities to perform the requirements of this contract, including any necessary GPOE and IT. GPOE means equipment normally found in a business office such as desks, chairs, typewriters, calculators, file cabinets, etc. IT means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes computers, ancillary equipment, software, firmware and similar products, services (including support services), and related resources.

H.7 Leasing

The Government contemplates leases of the following types: lease to ownership; lease with an option to purchase; and straight lease IT equipment. All leases may include integrated installation and warranty. Leasing terms and conditions and associated lease documentation will be established at the TO level.

If Government awards a TO for leased equipment it contemplates the use of the equipment for the entire term of the lease identified ("Lease Term"). However, the Lease Term of the lease agreement is from the date of acceptance of the equipment through September 30 of the fiscal year in which the TO is placed. Acceptance shall be defined in each TO. The lease, LTO or LTOP does not require, and should not be interpreted as requiring, either party to take any action or perform any covenant that is contrary to the Anti-Deficiency Act or other federal law. Accordingly, any TO for leased equipment shall not be deemed to obligate succeeding fiscal years or otherwise commit the Government to continue performance beyond the current Government fiscal year. Leases shall not exceed the TO period of performance.

H.8 Government Property, Information, Workspace

The Government may provide the items listed below as necessary for the Contractor to fulfill the tasks described in task order statements of work.

(a) Government Furnished Property (GFP). The Government may provide hardware and/or software requiring technical analysis, evaluation, verification, or study in support of a specific task. Such GFP will be specified in individual TOs. GFP provided to the Contractor in support of individual TOs shall be tracked through applicable procedures provided by the TO CO in accordance with the FAR. Property shall be accounted for and marked accordingly for identification and tracking purposes with the Contract Number, Task Order Number, Name of Resource assigned the equipment, Serial Number and other information as required by the TO CO. The Government does not intend to provide hardware/software equipment required to accomplish day-to-day work requirements in support of the overall contract-level effort. All GFP shall be returned to the Government at the completion of each TO unless otherwise specified.

(b) Government Furnished Information (GFI). The Government may provide information (e.g., technical data, applicable documents, plans, regulations, specifications, etc.) in support of a specific task. Such GFI will be specified in individual TOs.

(c) Government-Furnished Workspace. Such Government Furnished workspace will be specified in individual TOs.

H.8.1 Contractor Acquired Property.

In the event the Contractor is required to purchase property in the performance of this contract, compliance with the procedures of FAR Part 45 is required.

H.8.2 Disposition of Government Property

Thirty (30) calendar days prior to the end of the TO period of performance, or upon termination of the contract, the Contractor shall furnish to the TO COR a complete inventory of all Government Property in their possession under this contract that has not been tested to destruction, completely expended in performance, or incorporated and made a part of a deliverable end item. The TO COR will furnish disposition instructions on all listed property which was furnished or purchased under this contract.

H.9 Performance-Based Services Contracting (PBSC)

Through the direction of the Office of Management and Budget (OMB) Office of Federal Procurement Policy (OFPP), performance-based contracting techniques will be applied to task orders issued under this contract to the maximum extent practicable." For information about PBSC, refer to OFPP's Best Practices Handbook located at http://www.arnet.gov/Library/OFPP/BestPractices.

PBSC TOs must include at a minimum:

(a) Performance requirements that define the work in measurable, mission-related terms;

(b) Performance standards (i.e., quality, quantity, timeliness) tied to the performance requirements;
(c) A Government Quality Assurance Surveillance Plan (QASP) or other suitable plan that describes how the Contractor's performance will be measured against the performance standards or service level agreements (SLAs); and
(d) If the acquisition is either critical to agency mission accomplishment or requires relatively large expenditures of funds, positive and negative incentives tied to the performance standards/SLAs.

H.10 Conversion to a Performance Based Task Order

If both the Government and the Contractor agree, a TO can be converted from a term contract to a fixed price completion performance-based service contract after the initial period of performance. The conversion is accomplished as follows:

(a) Within ninety calendar days prior to the end of the TOs' initial period of performance, the Contractor shall prepare and submit for Government review, comment, and concurrence:

(1) A performance work statement (PWS) that captures all of the types of effort performed during the base year of performance, and
(2) A quality assurance plan (QAP). The QAP will address performance standards which relate to the performance requirements; how the Contractor's performance will be measured against the performance standards, and surveillance schedules and methods. The QAP may either be included as part of the PWS or as a separate document.

(b) Within sixty calendar days prior to the end of the TO's initial period of performance, the Government and the Contractor will resolve to their mutual satisfaction any comments or concerns on the PWS and/or QAP. Upon exercise of the option for the first follow-on period of performance, the Government has the unilateral right to modify the TO to incorporate the agreed to documents to accomplish the conversion to a performance-based contract.

H.11 Past Performance Evaluation

(a) Past performance information is relevant for future TO source selection purposes, regarding a Contractor's actions under previously awarded task orders under the same contract. It includes, for example, the Contractor's record of conforming to contract requirements and to standards of good workmanship; the Contractor's adherence to contract schedules, including the administrative aspects of performance; the Contractor's history of reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the Contractor's business-like concern for the interests of the customer. Past performance also includes the quality and timeliness of deliverables submitted to the Government in the delivery of its services.

(b) Upon completion of a TO base or option period, the TO COR will complete a TO evaluation via CPARs. The information will be used for future source selections under Evolve.

H.12 Disclosure of "Official Use Only" Information Safeguards

Any Government information made available or to which access is provided, and which is marked or should be marked "Official Use Only", shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Disclosure to anyone other than an officer or employees of the Contractor or Subcontractor at any tier shall require prior written approval of the TO Contracting Officer. Requests to make such disclosure should be addressed to the TO Contracting Officer and TO COR.

H.13 Disclosure of Information--Official Use Only

Each officer or employee of the Contractor or Subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed shall be notified in writing by the Contractor that "Official Use Only" information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to ten years or both.

H.14 Standard of Conduct at Government Installations

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity and shall be responsible for taking such disciplinary action with respect to his employees as may be necessary. The Contractor is also responsible for ensuring that his employees do not disturb papers on desks, open desk drawers or cabinets, or use Government telephones except as authorized.

Contractors shall not enter any Government employee's office space for which they are not authorized by that employee. Contractors shall not change their work location or use any government work desks for which they are not authorized by IRM/BMP/ITA/CM.

H.15 Advertisements, Publicizing Awards and News Releases

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity/ news release or commercial advertising without first obtaining explicit written consent to do so from the Evolve Program Manager. This restriction does not apply to marketing materials developed for presentation to potential government customers of this contract vehicle.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

H.16 Contractor Web Page

It is a material contract requirement that each Contractor maintain a publicly available webpage throughout the period of performance of the contract. The purpose of the webpage is for the Contractor to communicate with potential customers regarding the Contractor's ability to provide world-class professional support services for all DOS Program Offices. The webpage should demonstrate the functional capability associated with different products or business areas. The webpage should be easily accessible from the Contractor's front page, intuitive for novice computer users, and Section 508 compliant (See Section H.27). This webpage at minimum must include the following items:

(a) A copy of all TOs received under this contract (this can be a link to the "official government website");
(b) A list of the last three (3) years experience providing professional support services, listed by pool and DOS Program Office. The Contractor may also include a description of the products (deliverables) provided;
(c) Point(s) of Contact to provide information on customer satisfaction with the services performed;
(d) A description of the Contractor's quality assurance program;
(e) Point(s) of Contact for information related to IDIQ contracts;
(f) A list of any performance metrics or other methods used for tracking performance and their status;
(g) Teaming Coordinator's Point(s) of Contact; and
(h) Current list of Subcontractors.

The Contractor shall provide the EVOLVE Program Manager with the web address within ten (10) Government working days of receipt of the contract. The Contractor shall ensure all information provided on this web page is updated monthly.

H.17 Contractor's Employees Identification

During the period of this contract, the rights of ingress and egress to and from any office for Contractor's personnel shall be made available as deemed necessary by the Government. All Contractor employees, whose duties under this contract require their presence at any Government facility, shall be clearly identifiable by a distinctive badge furnished by the Government. In addition, corporate identification badges shall be worn on the outer garment at all times. Obtaining the corporate identification badge is the sole responsibility of the Contractor. All prescribed information shall immediately be delivered to the appropriate Government Security Office for cancellation or disposition upon the termination of employment of any Contractor personnel. All on-site Contractor personnel shall abide by security regulations applicable to that site.

All Contractor's shall include a signature in all email correspondence that identifies them as a contractor and the name of their company. During meetings and/or conference calls, all contractors shall identify themselves as contractors.

H.18 Teaming Arrangements

Because of the diversity of IT work contemplated under this contract, the Government anticipates that teaming will occur at the TO level, in response to specific TO requirements.

(a) Prime Contractors may subcontract with other Prime Contractors on an individual TO basis; however, the Government reserves the right to prohibit Prime Contractor teaming on an individual TO basis. If Prime to Prime teaming is prohibited it will be at the sole discretion of the Government.

(b) Teaming Coordinator. Each Prime Contractor shall provide an overarching Evolve Teaming Coordinator to serve as a single point of contact for prospective subcontractors and to continuously review the marketplace for companies that provide new and innovative products and professional services with which to subcontract. The Contractor is also encouraged to have non-exclusive access to multiple product and service providers.

H.19 Subcontracting

(a) In accordance with FAR 52.244-2 - Subcontracts, if the Contractor does not have an approved purchasing system, the Contractor shall obtain written contract level Contracting Officer consent prior to subcontracting under a:

(1) Cost-reimbursement, T&M or labor hour type contract; or
(2) Firm fixed price contract that exceeds $75 million.

(b)The subcontracting plan small business goals for large businesses under this contract are as follows:

Type of Business	Goal % of Total Planned Subcontracting Dollars
Small Business (SB)	
Small Disadvantaged Businesses (SDB)	
Women-Owned Small Businesses (WOSB)	
Service-Disabled Veteran Owned Small Business (SDVOSB)	
Veteran-Owned Small Business (included in SDVOSB)	
HUBZone	

(c) The Government reserves the right to require a subcontracting plan, as prescribed in FAR 52.219-9, at the task order level.

(d) The Contractor may add or delete Subcontractors without the express written consent of the Government. Although the Contractor can add or delete Subcontractors without express written consent of the CO, circumstances may exist in which regulatory approvals are required. An example is when a Contractor intends to subcontract with a Subcontractor that does not have an approved purchasing system. In such instance, CO approval must be received prior to subcontracting. With regard to any T&M task orders, any new Subcontractor approved for addition to the contract shall be reimbursed via the labor rates set forth in Section B. No additions or adjustments will be made to account for added Subcontractors.

H.20 Incorporation of Subcontracting Plan

The [insert Contractor name] subcontracting plan, dated [insert date], in response to the Evolve solicitation, and submitted in accordance with FAR 52.219-9, is hereby approved and incorporated herein.

H.21 Associate Contractor Agreements- TBD

H.22 Key Personnel

Key personnel are those Contractor personnel considered to be essential to the performance of the contract and TOs.

The Contractor's Program Manager, as described in Section G.2.4, is designated as key, and may only be replaced with the approval of the EVOLVE Program Manager and the CO, in accordance with the terms and conditions of Section H.23. The Contractor's Program Manager identified for this contract is:

NAME:
MOBILE TELEPHONE:
E-MAIL ADDRESS:

If the Government determines that certain personnel are "key" to successful completion of a TO, they will be designated as "Key Task Order Personnel" in the TO. Key Task Order Personnel are defined as follows:

(a) Personnel identified in the Task Proposal as key individuals to be assigned for participation in the performance of the TO and who may, at the discretion of the Government, be interviewed to verify resume representations;
(b) Personnel whose resumes were submitted with the TO Proposal; or
(c) Individuals who are designated as key personnel by agreement of the Government and the Contractor during TO negotiations.

H.23 Substitution of Key Personnel

The Contractor shall notify the TO CO and the TO COR prior to making any changes in Task Order Key Personnel. No changes in TO Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the TO Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The TO CO shall be notified in writing of any proposed substitution at least forty-five (45) days, or sixty (60) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

(a) an explanation of the circumstances necessitating the substitution;
(b) a complete resume of the proposed substitute; and
(c) any other information requested by the TO CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The Evolve Program Manager and the contract level CO will evaluate substitutions at the contract level and the TO COR will evaluate TO level substitutions. These individuals will evaluate such requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor. The Contractor shall allow a minimum of a two-week transition of key personnel.

H.24 Interrelationships of Contractors

(a) The Government has entered into other contractual relationships in order to provide technical support services in the conduct of studies, analyses, engineering, and other activities separate from the work to be performed under this contract, yet having links and interfaces to them. Further, the Government may extend these existing relationships or enter into new relationships. The Contractor may be required to coordinate with such other Contractor(s) through the Task Manager in providing suitable, non-conflicting technical interfaces and in avoidance of duplication of effort. By suitable tasking, such other Contractor(s) may be requested to assist the Government in the technical review of the Contractor's technical efforts. Information on reports provided under this SOW may, at the discretion of the Government, be provided to such other Contractor(s) for the purpose of such review.

(b) A Non-Disclosure Agreement (NDA), (Attachment TBD, *Non-Disclosure Agreement*), shall be signed by all Contractor employees assigned to perform services under a TO prior to any work commencing on the TO.

H.25 TBD

H.26 Insurance

Insurance of the following kinds and minimum amounts shall be furnished at any time at the request of the CO and maintained during the period of performance of this contract:

(a) Worker's compensation and employer's liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).

(b) General liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).

(c) Automobile liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c).

H.27 Information Technology Accessibility for Persons with Disabilities

All services and Electronic Information Technology (EIT) delivered as result of orders placed under this contract shall comply with accessibility standards in accordance with Federal Information Technology Accessibility as required by Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. Information about the Section 508 Electronic and Information Technology Accessibility Standards may be obtained via the Web at the following URL: from www.Section508.gov.

H.28 Notice of Internet Posting of Awards

DOS intends to electronically post the Evolve contracts, including fully-burdened labor rates, to the DOS internal web site. This does not include Contractor proposals or any other proprietary information provided by Contractors relevant to TO performance or by Offerors in response to the Evolve solicitation. Posting of the contract documents and associated modifications via the Intranet is in the best interest of the Government as well as the Contractors. It will allow Contractors to direct future customers to the site to view labor categories and rates as they develop their Independent Government Cost Estimates (IGCE) in preparation of proposed TOs.

H.29 Eventual On-Line Proposal and Ordering Capability

DOS hopes to establish an Intranet portal for the purpose of electronic and paperless TO processing. The Contractor will be required to support the electronic information requirements of the portal. The processing procedures and information requirements will be written into the contract at the time such capability is implemented. All contract deliverables and contract documentation will be centrally stored and maintained in the IRM/BMP/ITA/CM electronic contract portal.

H.30 Post Award Conference

The Contractor shall participate in a post award conference that will be held within ten (10) business days after contract award. The purpose of the post award conference is to aid both the Contractor and the Government in achieving a clear and mutual understanding of all contract requirements and identify and resolve potential problems (See FAR Subpart 42.5).

The CO is responsible for establishing the time and place of the conference and will notify the appropriate Government representatives and the Contractors. The Evolve Program Manager will designate or act as the chairperson at the conference. The chairperson of the conference shall conduct the meeting.

The conference may be conducted at a location within the Washington DC commuting area or completely online at the Government's discretion.

The Contractor further agrees to attend post award conferences on task orders as required. The TO post award conferences will establish work level points of contact for the TO, determine the TO administration strategy, roles and responsibilities and ensure prompt payment and TO close out.

H.31 Meetings/Conferences

Pre-award meetings or conferences may be necessary to resolve problems and to facilitate understanding of the technical requirements of the contract or task orders. All costs associated with the attendance at pre-award meetings/conferences shall be incidental to the contract and not separately billed.

H.32 Earned Value Management

In accordance with OMB Circular A-11, the Government will use Earned Value Management (EVM) to monitor tasks under EVOLVE. The Contractor shall provide EVM that meets the criteria as defined in the current American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-2002, *Earned Value Management Systems.*

Requires the contractor to abide by DoS Earned Value Management System Guidelines and American National Standards Institute/Electronic Industries Alliance Standard 748, *Earned Value Management Systems*, latest revision and to provide Control Account Plans and Earned Value Reports to designated Government and Contract program management staff for verification and validation purposes.

The Contractor shall use an Earned Value Management System (EVMS) to manage the task/delivery order that, at the time of task/delivery order award, has been recognized by the Contracting Officer (CO) as compliant with:

a. The guidelines in ANSI/EIA Standard -748 (current version at time of award).
b. The State Department's Earned Value Management Framework at the Third Level of Rigor, or as determined by the Department's IRM/BMP/ITA Office.
c. The data and reporting requirements of the Department's Electronic Capital Planning and Investment Control (eCPIC) System.

The Government anticipates the contractor's EVM system to feed data to a Government –owned system, once available. The contractor must provide accurate data to the government-owned system and reconcile output provided to the contractor from the government system. The Government's EVM system is the primary system and the contractor is required to directly participate by providing data into the Government's EVMS.

In the absence of a Government –owned EVMS, the Contractor shall use an earned value management system (EVMS) that complies with the criteria provided in ANSI/EIA-748, as described above, appropriately tailored to the task order and has been self-verified. If at any time during performance of the self-verification is determined to be defective, the Contractor shall correct the defect at no additional cost to the government.

Contractor and subcontractor participation is mandatory. The Contractor shall provide EVMS reports that include but are not limited to:

a. Using "Milestones Percentage Completed" as the predominant Earned Value methodology, and using a Work Breakdown Structure (WBS) jointly approved by the Government and the Contractor;
b. Providing, for each project, Project Plans that adhere to the Information Resource Management (IRM) Project Plan Template and including a detailed schedule with milestones;
c. Providing, for each WBS element, Control Account Plans (CAP) that follow IRM/BMP/ITA CAP Template and estimating the control account's planned resources, hours, materials, and milestones;

d. Providing a monthly status of all planned milestones with a variance analysis that reports the Cause, Impact and Corrective Action for all variances that are projected to reach or go beyond IRM's current EVMS thresholds (i.e., currently +/- 5%). The document shall follow IRM/BMP/ITA Milestone Status Template;
e. Recording time spent on DOS tasks daily into IRM/BMP/ITA time tracking system, once available, to determine the effort (labor hours) spent on each WBS element. All Contractors must "lock" the timecards (submit for Control Account Manager approval) twice a month to enable IRM/BMP/ITA to generate monthly EVM reports, including the Cost Performance Report (CPR);
f. Providing a schedule of performance-based payments by task and task/delivery order and report the actual payment amounts as incurred;
g. Providing all needed EVM data – to include labor hours, milestones, material costs, other direct costs (ODCs), and performance-based payment data – by the third business day of the month to facilitate monthly EVM report generation;
h. Providing, for Cost or Time and Material Contracts, billable rates to facilitate EVM report generation; and
i. Ensuring that all of the contractor's subcontractors comply with the EVMS requirements of the task/delivery order.

(a) The Government requires integrated baseline reviews. Such reviews shall be scheduled as early as practicable and should be conducted within 60 calendar days after (1) task order award, (2) the exercise of significant task order options, or (3) the incorporation of major modifications. The objective of the integrated baseline review is for the Government and the Contractor to jointly assess areas, such as the Contractor's planning, to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

(b) The Contractor shall provide the Contract Performance Report in accordance with the requirements of the task order.

(c) The Contractor shall provide an Integrated Master Schedule as part of each EVMS report.

(d) The Contractor agrees to provide access to all pertinent records and data requested by the TO Contracting Officer, IRM/BMP/ITA or duly authorized representative to validate and verify the accuracy and completeness of the EVMS data.

H.33 Organizational Conflict of Interest (If applicable on a task order)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting _____ (*description to be included in task order request*) _____.

(b) If any such conflict of interest is found to exist, the TO Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract

with the offeror and include the appropriate provisions to mitigate or avoid such conflict in the task order awarded. After discussion with the offeror, the TO Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents to the best of its knowledge that:

____(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this task order, or
____(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation/Waiver. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the offeror shall submit a mitigation plan to the Government, IRM/BMP/ITA/CM, for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.

(e) Other Relevant Information: In addition to the mitigation plan, the TO Contracting Officer may require further relevant information from the offeror. The TO Contracting Officer will use all information submitted by the offeror, and any other relevant information know to DOS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the TO Contracting Officer and Evolve Program Manager within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

H.34 Information Assurance (IA)

Information Assurance (IA) capabilities and actions protect and defend network availability, protect data integrity and provide the ability to implement effective computer network defense. As stipulated in individual Orders, the Contractor will provide cost effective, timely and proactive IA measures and controls including any required documentation. Corrective actions will be established and implemented to mitigate risks before exploitation and to protect against vulnerabilities and threats once they have been identified. Innovative approaches and best business practices are to be established and utilized for information system security.

The Contractor will comply with DOS information assurance requirements. These requirements may include but are not limited to: personnel security clearances/background checks; operations-

-security risk assessments, vulnerability of management processes and plans, installation/configuration of IA compliance documentation; and defense of the environment--including hardware and software, networks, and supporting infrastructure, as dictated by the nature of the information (classified/unclassified) and associated risk.

The Contractor must report Foreign Interests at the prime and subcontract levels as required by the task order. The Contractor must provide access to the Contractor's facilities, personnel and documents for the purposes of audit or inspection by an authorized Inspector General (IG) or designated security certification activity to ensure appropriate IA practices are in place. Contractor facilitates housing Government Systems or data might require Security Assessment and an ATO (authority to operate).

H.35 IT Security Considerations

IT Security, often referred to as cybersecurity, is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Examples of IT Security services include, but are not limited to:

(1) Continuous Diagnostics and Mitigation
(2) Continuous Security Monitoring Services
(3) Identity Management and Access Management
(4) Information Assurance
(5) Intrusion Detection
(6) IT Disaster Recovery Services
(7) IT Security Incident Response
(8) Network Security Monitoring
(9) Security Assessment Services / Vulnerability Analysis Services
(10) ATO status and the Authorization and Accreditation of Systems
(11) Asset Inventory and Management
(12) Overall IT Security posture of the Agency from the network and applications to the end points.

Contractors will be subject to IT security standards, policies, reporting requirements, and government wide laws or regulations applicable to the protection of government wide information security, as listed in Attachment J-TBD, Cybersecurity & Supply Chain Risk Management.

H.36 Additional Cybersecurity and Supply Chain Risk Management (SCRM) Requirements

Cybersecurity and SCRM are dynamic areas with developing regulations and requirements as evidenced by the publication of the Cybersecurity Maturity Model Certification (CMMC) framework by the Department of Defense (DoD) in January 2020 as well as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 and SP 800-171. It is important for the vehicle to remain relevant in light of changing requirements (see Attachment J-TBD: Cybersecurity & Supply Chain Risk Management (SCRM) References).

H.37. Accreditation

Contractors should begin preparing for CCM and SCRM accreditation by staying aware of developing requirements and by implementing the appropriate NIST SP 800-series documents. Examples of appropriate actions include the following:

(1) Review your company's current compliance with NIST SP 800-171 Rev 1 in relationship to your expected CMMC level requirements. Begin drafting a System Security Plan (SSP) in accordance with NIST SP 800-18 Rev 1, (the SSP is generated in accordance with the Risk Management Framework as outlined in NIST 800- 37 r2) If you currently have a Plan of Action and Milestones (POAM) in place or identify additional concerns, dedicate appropriate resources to ensure that progress is being made to close any gaps as quickly as possible. Examine Draft NIST SP 800-171B for enhanced security requirements to improve cybersecurity maturity capabilities as applicable given the CMMC level you intend to attain.
(2) Review your company's current compliance with NIST SP 800-161 to include the establishment of a SCRM Plan.
(3) Investigate your subcontractor base as SCRM requirements may flow down to subcontractors, including commercial item subcontractors. It is expected that consent to subcontract at the Order level may also consider subcontractor CMMC level.
(4) Participate in SCRM and/or CMMC workshops recommended or hosted by DOS.

H.38 Off Ramping -TBD

H.38 Onboarding –TBD

H.39 Cybersecurity Maturity Model Certification (CMMC) and Other Certifications

DOS reserves the right to survey and assess Evolve awardees from time-to-time in order to identify and to publicly list each industry partner's CMMC level and ISO certifications, such as, but not limited to, ISO/IEC 27010:2015, ISO/IEC 20243, ISO/IEC 27000, ISO/IEC 27036 and ISO 9001:2015.

Evolve Order competitions may be restricted by designation of an applicable CMMC level and / or ISO certification, such as, but not limited to, ISO/IEC 27010:2015, ISO/IEC 20243, ISO/IEC 27000, ISO/IEC 27036 and ISO 9001:2015.

DOS reserves the right to require CMMC Level 1 certification as mandatory to be considered for an Evolve option as well as for any general Open Season or targeted onboarding opportunities.

(End of Section H)

SECTION I - CONTRACT CLAUSES

I.1 Clauses Incorporated By Reference- TBD

I.2 Security Requirements For Unclassified IT Resources (custom clause)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DOS network or operated by the Contractor for DOS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DOS unclassified systems that directly support the agency's mission. The security requirements include, but are not limited to, how the Department of Homeland Security's sensitive information is to be handled and protected at the Contractor's site, (including any information stored, processed, or transmitted using the Contractor's computer systems), the background investigation and/or clearances required, and the facility security required. This requirement includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DOS with significant replacement cost should the contractor's copy be corrupted; and
(2) Access to networks or computers at a level beyond that granted the general public, (e.g. such as bypassing a firewall).

(b) At the expiration of the contract, the contractor shall return all sensitive DOS information and IT resources provided to the contractor during the contract, and a certification that all DOS information has been purged from any contractor-owned system used to process DOS information. Organizational elements shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(c) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), and the Government Information Security Reform Act of 2000, and the Federal Information Security Management Act of 2002. The plan shall meet IT security requirements in accordance with Federal policies and procedures that include, but are not limited to OMB Circular A-130, Management of Federal Information Resources, Appendix III, and Security of Federal Automated Information Resources;

(d) Within _*_days after TO award, the contractor shall submit for approval an IT Security Plan. This plan shall be consistent with and further detail the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document. **to be specified on a TO basis*.

(e) Within 6 months after contract award, the contractor shall submit a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. When accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The contractor shall comply with the approved accreditation documentation.

I.3 Notification Of Ownership Changes (FAR 52.215-19)

I.4 TBD

I.5 TBD

I.6 Determination of Award Fee

***Task Orders Only-If Applicable**

(a) The Government shall evaluate contractor performance at the end of each specified evaluation period(s) to determine the amount of award. The contractor agrees that the amount of award and the award fee methodology are unilateral decisions to be made at the sole discretion of the Government.

(b) Contractor performance shall be evaluated according to a Performance Evaluation Plan. The contractor shall be periodically informed of the quality of its performance and areas in which improvements are expected.

(c) The contractor shall be promptly advised, in writing, of the determination and reasons why the award fee was or was not earned. The contractor may submit a performance self-evaluation for each evaluation period. The amount of award is at the sole discretion of the Government but any

self-evaluation received within (insert number) days after the end of the current evaluation period will be given such consideration, as may be deemed appropriate by the Government.

(d) The Government may specify that a fee not earned during a given evaluation period may be accumulated and be available for allocation to one or more subsequent periods. In that event, the distribution of award fee shall be adjusted to reflect such allocations.

I.7 Performance Evaluation Plan [1]*

(a) A Performance Evaluation Plan shall be unilaterally established by the Government based on the criteria stated in the contract and used for the determination of award fee. This plan shall include the criteria used to evaluate each area and the percentage of award fee (if any) available for each area. A copy of the plan shall be provided to the contractor _____ (insert number) calendar days prior to the start of the first evaluation period.

(b) The criteria contained within the Performance Evaluation Plan may relate to: (1) Technical (including schedule) requirements if appropriate; (2) Management; and (3) Cost.

(c) The Performance Evaluation Plan may, consistent with the contract, be revised unilaterally by the Government at any time during the period of performance. Notification of such changes shall be provided to the contractor_____ (insert number) calendar days prior to the start of the evaluation period to which the change will apply.

I.8 Distribution of Award Fee [2]*

(a) The total amount of award fee available under this contract is assigned according to the following evaluation periods and amounts:

Evaluation Period:
Available Award Fee:
(insert appropriate information)

(b) Payment of the base fee and award fee shall be made, provided that after payment of 85 percent of the base fee and potential award fee, the Government may withhold further payment of the base fee and award fee until a reserve is set aside in an amount that the Government considers necessary to protect its interest. This reserve shall not exceed 15 percent of the total base fee and potential award fee or $100,000, whichever is less.

(c) In the event of contract termination, either in whole or in part, the amount of award fee available shall represent a pro rata distribution associated with evaluation period activities or events as determined by the Government.

[1] Task Orders Only if Applicable
[2] Task Orders only if applicable

(d) The Government will promptly make payment of any award fee upon the submission by the contractor to the contracting officer's authorized representative, of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without using a contract modification.

I.9 Performance-Based Payments (FAR 52.232-32)

I.10 Qualifications Of Contractor Employees- TBD

I.11 Contractor Personnel Screening For Unclassified IT Access - TBD

(End of Section I)

SECTION J – LIST OF ATTACHMENTS

TBD

(End of Section J)

SECTION K - REPRESENTATIONS AND CERTIFICATIONS

TBD

(End of Section K)

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

L.1 Solicitation Provisions Incorporated by Reference- TBD

L.2 Set Asides for Pools

Only Pool 3 is set-aside as a total small business set-aside. Pools 1, 2, 4, and 5 are "full and open."

L.3 Type of Contract

The Government contemplates award of multiple IDIQ contracts resulting from this solicitation. The contracts plans to primarily utilize T&M, LH and FFP TOs but reserves the right to use any type of contract described in FAR 16. Incentive and award fee provisions may also be applied to individual task orders.

L.4 Service of Protest-TBD

L.5 Proposal Schedule

All proposals are due NO LATER THAN 2:00 P.M. Eastern Standard Time on the date specified on the SF-33 (RFP Section A).

CAUTION: See the proposal submission instructions, including the provision describing treatment of late submissions, notifications and withdrawals of proposals at FAR Clause 52.215--1 Instructions to Offerors—Competitive Acquisition.

L.5.1 Communications and Questions

Communications and questions concerning this solicitation or requests for clarification shall be made in writing to the Contracting Officer. The due date for communications and questions concerning the RFP is TBD.

As soon as an Offeror is aware of any problems or ambiguities in interpreting the specifications, terms or conditions, instructions or evaluation criteria of this solicitation, the Contracting Officer shall be notified.

Questions shall be submitted via e-mail to _____. Electronic mail attachments, if included, shall be prepared using Microsoft Word.

When submitting questions and comments, please refer to the specific text of the RFP in the following format:

Subject: RFP No. _____
Reference: RFP Section ___, Paragraph(s) ____, Page(s) ____.

All questions will be answered via amendment and provided to all Offerors on the Internet at www.fbo.gov and will not attribute the questions to the submitting Offerors.

L.5.2 Delivery of Proposal

The proposal shall be delivered via TBD and shall be entitled Contractor Name Evolve DOS Solicitation Number: TBD

L.6 Total Number of Pool Awards

During the bidding process, offerors may bid on one, many or all functional pools. If selected for award on Pool 1 – IT Management, the offeror, to include any proposed subcontractors, will not be eligible for award on any of the other functional pools. The government intends to award Pool 1 first. DOS will contact any offeror selected for award on Pool 1 that is also in line for award on any other pool. Offerors will have the choice to accept an award for Pool 1 and waive their rights to an award for Pools 2-5.

For Pools 2-5, no one offeror (aka the prime contractor), may receive more than two awards. The two award limitation also applies to subsidiaries that fall under the same parent company or corporate umbrella and to any JV or Mentor-Protégé relationships. The government will not award more than two pools to any combination of offerors that belong to the same underlying entity.

In the event multiple offerors submit proposals that are in contention for award on two or more of the same pools for pools 2-5, the Government reserves the right to select which two pools an offeror may receive. Offerors who submit multiple proposals shall clearly rank which pools they wish to be awarded by filling out the chart below and submitting it with their cover letter for phase 2. An offeror's overall evaluated price, technical rating and pool preference may be considered in determining which two pools an offeror receives. The final decision will be based on what's in the best interest of the government at the time of award.

Rank	***Preference for Pool Award (list pool in descending order of preference)***
1	*(list pool 2-5)*
2	*(list pool 2-5)*
3	*(list pool 2-5)*
4	*(list pools 2-5)*

The government intends to award up to 6 IDIQs per pool.

L.7 Proposal Preparation Costs

This RFP does not commit the Government to pay any cost for the preparation and submission of a proposal in response to this RFP. The Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds in connection with this procurement.

L.8 Small Business Classification Code for Pools Three

(a) For purposes of this solicitation and each resultant contract, North American Industry Classification System (NAICS) codes will be established at the Functional Category-level. Under these classifications, a concern is considered a small business if its average annual receipts for its preceding three fiscal years do not exceed the size standard.

Pool	Description	NAICS Code and Description
3	Data Processing, Hosting, and Related Services	518210

Subcontracted work should be classified under the NAICS code appropriate for the type of work (See FAR Part 19 for NAICS code size standards).

L.9 General Instructions

Offerors shall examine and follow all instructions. Failure to do so may result in the proposal being determined to be unacceptable and removed from consideration for award. Proposals shall conform to solicitation provision FAR 52.215--1 Instructions to Offerors - Competitive Acquisition and be prepared in accordance with this section.

To aid in the evaluations, proposals shall be clearly and concisely written as well as neat, indexed (cross -indexed as appropriate) and logically assembled. Prospective Offerors are asked to bear in mind that all material submitted should be directly pertinent to the requirements of this RFP. Extraneous narratives, elaborate brochures, uninformative "PR" material and so forth, shall not be submitted. All pages of each part shall be appropriately numbered, and identified with the name of the Offeror, the date, and the solicitation number to the extent practicable.

L.9.1 Proposal Integrity

In responding to this RFP, it is the Offeror's responsibility to provide current, complete, and accurate information in their proposal. If in reviewing the proposal the Government identifies or otherwise learns that the provided proposal information is not accurate or misrepresents the Offerors status or capabilities, that information may be used by the contracting officer as part of the Offeror's responsibility determination and could result in the offeror not being eligible for award.

L.9.2 General Format Instructions for Written Portion of the Proposals

Offerors shall furnish the proposal in two separate electronic volumes, Technical/Management (Phase One and Phase Two) and Pricing in the quantities specified below. Each volume shall be complete in itself in order that evaluation of one volume may be accomplished independently of, and concurrently with, evaluation of the other. Electronic copies shall be formatted using Microsoft Office with file names that are consistent with the structure of the proposal. Individual file sizes shall not exceed 5 MB.

The font shall be 12-point Times New Roman. No reduction is permitted except for organization charts or other graphic illustrations. In those instances where reduction is allowable, Offerors shall ensure that the print is easily readable; no less than 8-point font on graphs and 10-point font on tables. Each page shall have adequate margins on each side (at least one inch) of the page. Header/footer information (which does not include any information to be evaluated) may be included in the 1" margin space. Offeror's proposals shall not exceed the page limitations set forth in L.10.1. Pages that exceed the maximum page limitation will not be evaluated.

L.10 Number of Proposals an Offeror Can Submit

The Evolve source selection will be conducted at the Pool level. The proposal must demonstrate the offeror's ability to provide the full range of IT services and solutions within the Pools selected. The Offeror shall organize its proposal to clearly distinguish the individual Pool(s) proposed.

Offerors' proposals submitted under Pool Three, a total small business set-aside must meet the small business size standard (See Section L.8). While offerors can submit proposals for all pools they will not receive awards for all pools (See Section L.6).

L.10.1 Pool One- Full and Open Competition

Pool One: Minimum Criteria (Go/No-Go)

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offerors not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. Offerors unable to substantiate meeting all Go/No-Go criteria will not receive further consideration and their Phase 1 response will not be reviewed.

Minimum Criteria	Instructions Language
Security Clearances	Offerors shall possess, and provide proof of, a valid Top Secret Facility Clearance or higher at the time of proposal submission. Offerors shall certify their ability to submit all key personnel cleared at the Top Secret or Secret level for reciprocity on Day 1 at time of proposal Offerors shall submit their DD254 at time of proposal.
Pool One - Certifications	Offerors shall be certified, and the Proof must be provided with Phase 1 submission. Offerors shall provide proof of the following certifications with their Phase 1 submission: 1. CMMI Development — Level 3 or higher 2. CMMI Service — Level 3 or higher 3. ISO 9001 certified
NDAA Compliance	Completed Express NDAA Certification in support of the John S. McCain National Defense Authorization Act Fiscal Year 2019 (Pub. L. 115-232). Paragraph (a)(1)(B) of section 889 in accordance with FAR 52.204-26, Covered Telecommunications Equipment or Services Representation and/or other appropriate documentation that it does not provide covered services or supplies as defined by the NDAA

Intent/Cover Letter	A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government, including which Pools it intends to bid on. The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least 180 calendar days from the date of receipt by the Government.
Small Business Subcontracting Plan	

Pool One: Factor One — Primary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below

- Adhere to prescribed page limits.
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Zero Trust Model

Problem Statement: Transformation to digital platforms and emerging changes such as 'working from home' and migration of agency digital assets to multiple commercial cloud environments have changed the digital boundaries of the U.S. federal government workspace. Solutions previously put into place to secure the perimeter have become inadequate to respond to increasing demands for access from anywhere and everywhere. This is coupled with increases in data and security breaches that can lead to an environment in which one can never trust and needs to always verify.
As a result, the DOS requires a strategic initiative to architect an enterprise Zero Trust Model (ZTM) that will prevent data breaches from occurring and protect DOS assets by assuming no entity can be trusted. This ZTM solution needs to ensure that anything and everything is adequately verified before granted access to network devices, management systems, applications, and sensitive data from anyone, including remote worldwide employees. The ZTM must be scalable, agile, and developed to cover assets, services, data, etc. located in several on-premises data centers owned by DOS and in multi-cloud environments for a hybrid, large enterprise network.

Challenge: Propose a strategic solution that also ensures the ZTM contains no duplicative products, establishes a priority focus of implementation, outlines a realistic timeline of milestones, and provides centralized logging and reporting for analytics of activity.
Describe your phased approach to transform a distributed worldwide computing environment hosting many bureau-managed systems in various stages of maturity and varying levels of data sensitivity into an environment supporting the ZTM.
The solution should be scalable and agile such that it secures, protects, detects, and defends against cybersecurity threats for a hybrid, large enterprise network with a global remote workforce and enforces accurate, least privilege per-request access to information systems and services in a networked environment assumed to be compromised. Additionally, the proposed solution should meet these minimal requirements:

- Do not allow implicit trust for anyone or anything attempting to connect to key networks, systems, data or other resources;
1. Explicit authentication and authorization should be made before allowing access, followed by continuous monitoring for changes;
2. Be able to detect and effectively respond to anomalous activities in real-time; and
3. Enable comprehensive visibility, analytics and proactive response actions across the entire communications access and security infrastructure.

Assumptions: The on-premises IT infrastructure is primarily composed of Cisco devices. The primary authentication is Microsoft Active Directory and Okta for applications hosted in the cloud. Roughly 75-85% of DOS's employees work remotely using various government and personally owned mobile devices.

Format/Instructions: Develop a white paper of no longer than three (3) pages; Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.
The Offeror's submission shall include the following artifacts: project plan, discovery activities, migration strategies, risk mitigation plans, and limited impact on operations approach.

FITARA-FISMA/Cyber Scorecard Improvement

Problem: As detailed on the FITARA scorecard, DOS earned a score of D for FISMA (Cyber). It is not alone and, in general, the government is struggling to implement FISMA across the board.

Challenge: DoS has set a lofty goal of achieving an A score in the next 12 months for FIMSA on the FITARA scorecard. How would you enable this goal to be realized? Be sure to provide an understanding of FISMA and any assumptions made.

Assumptions: None.

Format/Instructions: Develop a white paper of no longer than three (3) pages; Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.
The Offeror's submission shall include the following artifacts: project plan, discovery activities, migration strategies, risk mitigation plans, and limited impact on operations approach.

Pool One: Factor Two — Past Experience and Past Performance

Part One: Past Experience Submission

The Offeror must demonstrate relevant experience by submitting five (5) Relevant Experience Projects (REPs) as follows:

a) One (1) for Enterprise Architecture that includes migration to the cloud
b) One (1) for Zero Trust Architecture
c) One (1) for Portfolio Management and Capital Planning
d) One (1) for Process Improvement
e) One (1) for Budget and Financial Management.

Use the REP Template in accordance with the instructions herein.

A REP may consist of a contract or task order issued against an IDIQ or BPA; but simply holding an IDIQ contract or BPA is not sufficient. The Offeror must have performed work on a task order issued against the contract or BPA.

Using the REP Template, the Offeror shall identify five recent and relevant Government and/or commercial efforts on which it has performed as the prime contractor.

In a ***one-page addendum attached to each REP***, the Offeror shall:

1. Describe which of the five areas the past experience demonstrates and why.
2. Include a description of how the Offeror's past performance demonstrates their capability and capacity to deliver high quality service and solutions in a performance-based environment.
3. Focus on the key requirements of the project, as well as the size, scope and complexity of the efforts, the relevance to the pool the performance is being submitted for and if applicable, the performance measures and service level metrics applied to specific program objectives, and the actual results achieved against those measures. The service-level agreements or performance standards should be specific and show the target performance levels that are set forth under the applicable contracts.
4. A summary of performance ratings shall be provided showing the performance results achieved by the prospective Offeror for the latest two contract rating periods.

Part Two - Past Performance Assessment (CPARS past performance record or Attachment J-8) for each Relevant Experience Project

For each REP, the Offeror must submit the associated past performance assessment. Acceptable forms of past performance assessments are data contained in Contractor Performance Assessment Reporting System (CPARS) or a Past Performance Survey *(Attachment J-8).*

The Offeror must demonstrate favorable past performance for each project submitted as a REP. The burden of providing thorough, organized and complete past performance information rests with the Offeror. Failure to submit qualifying past contractual performance information when it exists will be deemed a material nonconformity and result in the offer being summarily rejected.

Favorable past performance is defined as: each past performance assessment receiving a satisfactory or better rating for the majority of rated elements. The Offeror will not be evaluated favorably or unfavorably on past performance in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available. Offerors will assume DOS has no past performance records at hand and that no member of DOS has personal knowledge of the Offeror's past performance.

Commercial vs. Federal Past Performance: DOS will consider commercial and federal past performance equally. DOS reserves the right to verify past performance information and may use broad discretion in considering additional past performance sources. DOS retains the right to validate the sources and content of past performance information.

Past Performance (when CPARS information exists): If interim or final ratings exist in CPARS for the submitted project, the Offeror must provide a copy of this rating with their proposal. If a final rating is not available, the most current past performance information will be used.

Past Performance (when CPARS information does not exist): The Offeror may ONLY submit Attachment J-8, Past Performance Survey in the event CPARS information is not available. If CPARS information is available for any submitted REP, it must be used for the Past Performance evaluation.

If the project(s) are considered Non-U.S. Federal projects, the Offeror must submit a Past Performance Survey using the template in Attachment J-8, "Past Performance Survey." No other format or additional proposal documentation will be considered.

Using the Past Performance Survey in Attachment J-8: the Offeror will provide the survey directly to each of the references. The Past Performance Survey must be completed and signed by a Contracting Officer, or Contracting Officer's Representative, or Contracting Officer's Technical Representative with cognizance over the submitted project. For a commercial project, the Past Performance Rating Form must be completed and signed by a Corporate Officer/Official of the customer with cognizance over the submitted project.

The Offeror will instruct each rater to send a completed form directly back to the Offeror. The Offeror must submit all Past Performance Rating Forms, as applicable, with their proposal submission.

Misleading Information: In the event the evaluation team discovers misleading, falsified, and/or fraudulent past performance ratings, the Offeror will be eliminated from further consideration for award. Falsification of any proposal submission, documents, or statements may subject the Offeror to civil or criminal prosecution under Section 1001 of Title 18 of the United States Code.

Adverse Past Performance Narrative (***Optional one-page***): An Offeror may submit a one-page narrative for each project being used for past performance to provide information on problems encountered on the submitted projects and the Offeror's corrective actions. This submission is not required but may be included to address past performance assessments where the majority of rating elements are below satisfactory. The Government will consider this information, as well as information obtained from any other sources, when evaluating the Offeror's past performance.

Pool One: Factor Three — Secondary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below

- Adhere to prescribed page limits

- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

- Offerors shall be prepared to give all oral presentations during the same day with brief breaks in-between and in sequential order as listed below.

Challenges in this section:

IT Management Challenges

- Managing Communications and Change Management
- Responding to Legislative and Federal Policy Updates
- Enterprise Asset Hardware, Software Inventory and Control
- Growing a Professional Cadre of IT Program and Project Managers

Strategic Planning Challenges

- Business Management and Planning
- Managing Communications and Change Management

Cybersecurity Challenges

- Cloud Platform Security Management Automation
- Domain Name, Email System and Web Governance

Financial Management Challenges

- Monitoring Performance in a Mixed Portfolio
- Collecting Data to Address Management Priorities and Reporting Requirements

Enterprise Architecture Challenges

- Advisory Services
- Solution Architecture with Focus on Cloud Computing
- Cybersecurity Architecture
- Technology Assessment

Innovation Challenge

- Innovation Roadmap

Pool One: Factor Four — Cybersecurity Approach

Part One — Supply Chain Risk Management (4 pages)

The Offeror shall describe its approach to supply chain risk management and, at a minimum, address:

1. Specific practices currently in place to reduce supply chain risk.
2. Actions taken to identify, manage and mitigate supply chain and cybersecurity risk.
3. Approach to mitigating and/or eliminating the risk of sabotage, maliciously introduced unwanted function, or other subversion to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of devices delivered to the Government.
4. The Offeror's intention regarding obtaining CMMC, the target certification level, and a tentative timetable for attaining it.
5. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror, to include ISO certifications (e.g., ISO/IEC 27001:2013, ISO 28000:2007 and ISO 9001:2015).
6. A narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services.
7. Actions taken to mitigate widespread supply chain sabotage when it occurs within the production environment. Describe how to contain and remove the threat while minimizing operational impacts.
8. Approach to managing sourcing risks as an integral part of enterprise architecture planning and design.

Part Two — Cybersecurity History (4 pages)

The Offeror shall describe its cybersecurity history and, at a minimum, address:

1. Number of Cybersecurity violations, infractions, or concerns in the last 5 years. Include date, summary and mitigation. This includes any violations from subcontractors working with or on behalf of.
2. Cybersecurity violations planning. Provide a plan on how the company will address cybersecurity violations, infractions or concerns.
3. Systems Assessed in the last 5 years. Include timelines, summaries, ATO and POA&M status for systems developed or implemented by the vendor in government environments.
4. For any system requiring connection to the Department's infrastructure or requiring access to federal information or data, provide a self-assessment using NIST SP 171 for each system.
5. Positions that would require elevated access to the Department's infrastructure. Provide a summary of the process in which these personnel would be managed, to include any training provided by the company or expected by the government to provide in order to maintain federal cyber hygiene standards. Additionally provide anything needed by the government to assist with these processes.

6. If planning to develop any technology for the government, provide a plan on how the software and/or hardware will be secured. Include how federal cyber hygiene standards and NIST requirements will be obtained and maintained.

Pool One: Factor Five — Management Approach

Program Management - 4 pages

The Offeror shall describe its proposed management structure, the position within the overall corporate organization of the division or group proposed to perform this effort, and the level of corporate project oversight planned in terms of authority to make programmatic decisions and implement design solutions. In addition, the Offeror shall provide the resume of the proposed Program Manager (PM). If the proposed PM is not a current employee, then the resume must include a statement that the prospective employee has authorized his/her resume to be submitted, intends to accept employment if the Contractor is selected for award and that the parties have discussed salary parameters. If the PM candidate becomes unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The Offeror shall also describe its management solution including the following topics:

1. The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the tasks awarded under this contract.
2. The proposed Project Management approach and the Offeror's methodology for ensuring cost, schedule and performance objectives (including service-level agreements or other types of performance metrics and measures) are controlled, reported, and managed.
3. The approach for managing multiple task orders for this effort, including:
    a. The tools and methodologies for planning the activities of its team(s),
    b. Scheduling, organizing, and deploying resources,
    c. Controlling of task execution, monitoring progress, status reporting, resolving critical issues, and planning for subsequent phases of work. Earned Value Management.
4. The Offeror's proposed Earned Value Management System (EVMS), its level of compliance with ANSI/EIA-748, and its ability to capture and evaluate cost, schedule, risk, and performance data throughout the life of a task.
5. The governance and reporting structure and the degree to which it provides transparency and Government access to real time cost, schedule and performance metrics

Quality Control Solution - 2 pages

The Offeror shall describe its Quality Control solution and how it relates to DOS' objectives stated in Section C. The Offeror's Quality Control solution shall include the following information:

1. A description of the Quality Control review/audit process, documentation of the process, methods of internal review, participants in the review and the frequency of review.
2. A description of the approach and procedures for handling corrective actions.

Recruitment, Retention, and Training- 3 pages

The Offeror shall describe actions it takes to recruit, train, and retain high-quality personnel, including a description of its processes, procedures, and policies. Of particular interest is the demonstration of an innovative methodology rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract.

Using *Attachment J-5, Staffing Levels Profile Form*, the Offeror shall provide the number of personnel currently in place within the cognizant business unit (i.e., the legal entity proposing on this procurement), the number of personnel with security credentials, the education and professional certifications obtained by the workforce, their average length of service, and the turnover rate experience of the workforce for last three (3) year period. The turnover rate is defined as the number of personnel who departed (regardless of reason) divided by the total number of personnel at the end of the period. *(This matrix is excluded from the page limitations)*

In the summary page provide a count of current employees aligned to current positions held and the duration employed (prime and teaming partners). Each employee shall be referenced in a single position that is currently held by that individual.

Using *Attachment J-6, Labor Category Table*, the Offeror shall describe the personnel qualifications and experience for each of its labor categories, including a crosswalk with the Government's labor categories and the associated education and experience.

Pool One: Factor Six — Ability to Achieve Results Through Teaming

In 3 pages, the Offeror shall describe its approach to developing relationships with subcontractors and teaming partners, and specifically how it will continually provide DOS with the best sources of solutions and services. The Offeror's response should demonstrate not only a systematic approach to identifying the most relevant and modern technologies, services, and techniques available in the marketplace, but should also discuss their approach to integrating various subcontractors and teaming partners to successfully meet the Department's objectives as described in task order requirements.

L.10.2 Pool Two- Full and Open Competition

Pool Two: Minimum Criteria (Go/No-Go)

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offerors not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. **Offerors unable to substantially meet all Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed**.

Title of Evaluation Factor	Language
Security Clearances	Offerors shall possess, and provide proof of, a valid Top Secret Facility Clearance or higher at the time of proposal submission. Offerors shall certify their ability to submit all key personnel cleared at the Top Secret or Secret level for reciprocity on Day 1 at time of proposal Offerors shall submit their DD254 at time of proposal.
NDAA Compliance	Completed Express NDAA Certification in support of the John S. McCain National Defense Authorization Act Fiscal Year 2019 (Pub. L. 115-232). Paragraph (a)(1)(B) of section 889 in accordance with FAR 52.204-26, Covered Telecommunications Equipment or Services Representation and/or other appropriate documentation that it does not provide covered services or supplies as defined by the NDAA
Pool Two- Certifications	Offerors shall be certified, and Proof must be provided with Phase 1 submission. Offerors shall provide proof of certification with their Phase 1 submission per pool. 1. CMMI Development — Level 3 or higher 2. ISO/IEC 27001 3. Proof that the contractor can obtain the required Consolidation Receiving Points in the National Capital Region (NCR) to ensure proximity to the Department's State Annex-21 (SA21) located at 7500 Boston Blvd., Springfield, VA, 22153
Intent/Cover Letter	A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government, including which Pools it intends to bid on. The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least 180 calendar days from the date of receipt by the Government.

Small Business Subcontracting Plan	

Pool Two: Factor One — Primary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below
- Adhere to prescribed page limits
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Modernize Network and Infrastructure
Problem Statement: DOS has varying refresh cycles for their systems: workstations, networking hardware, radio systems, PBX/communications servers, and infrastructure. There is a constant need to upgrade or replace current equipment or infrastructure while maintaining compatibility with existing functionality/services and with minimal disruption to the current work environment. **Challenge:** Develop a high-level, phased project plan to replace networking hardware, i.e., distribution and access switches, and infrastructure (cabling: horizontal and vertical, to include consolidation at a main terminal space and building ingress/egress through a telecommunications service entrance facility) in a multi-story active workplace. **Assumptions:** Within reason, the installation team will have full cooperation from the embassy to adapt to the installation team's needs. Additionally, engineering and design services are not needed as that will have already been completed. This is an implementation task. Finally, the installation approach must have minimal impact on current embassy operations. **Format/Instructions:** Develop a white paper of no longer than three (3) pages. This must include proposed architectural drawings. Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.

Pool Two: Factor Two — Past Experience and Past Performance

Part One — Past Experience Submission

Offerors shall read each of the following scenarios and follow the instructions for developing a case study relevant to each scenario to demonstrate recent and relevant experience. Offerors shall

submit up to two (i.e., no less than one, no more than two) case studies for evaluation by the Government per scenario.

Scenario One: Network Service Design and Implementation

Each case study will be no more than 3 pages and must include the total number of wide-area networks designed and implemented into production on a global scale equivalent to 163 embassies and 93 consulates around the world and demonstrate recent experience (within the past three (3) years immediately prior to the date of solicitation). The total dollar amount shall be provided yearly per project implementation and the Offeror shall provide Network Architecture Diagrams & the SOW with relevant, highlighted sections.

Network Services Design and Implementation — artifacts must demonstrate:

1. How the Offeror configured and deployed a scalable WAN on a global scale where sites have different requirements
2. How the Offeror improved an organization's network capacity and performance without taking on huge costs
3. How the Offeror provided network security and performance for users in an access-anywhere unified network that requires zero-trust security policies to protect sensitive government information, while providing employees with easy access to business-critical applications and files.

Scenario Two: Infrastructure

Each case study will be no more than 3 pages and must include a description of how the Offeror updated infrastructure to be more efficient, effective, secure, and aligned with industry standards. In alignment with BICSI standards, this will entail the install, labeling, testing, underground duck bank infrastructure, backbone and horizontal cable implementations, and documentation. The time period covered by this needs to be within the past three (3) years immediately prior to the date of solicitation. The total dollar amount shall be provided yearly per project implementation and the Offeror shall provide Network Architecture Diagrams & the SOW with relevant, highlighted sections.

Infrastructure — artifacts must demonstrate:

1. A diagram documenting your approach. Solutions should accomplish the following:
    - Optimize workloads, maximize efficiency, and build a resilient system
    - Leverage enterprise emerging trends and technologies while ensuring a balance with operational stability
2. Key written takeaways summarizing your approach. Be sure to address the following in your approach:
    - Balances the need to innovate while "keeping the lights on"
    - Keeps costs down and optimizes operational costs, both on-premises and off, while ensuring flexibility and scalability for future requirements

Scenario Three: Overseas Turnkey Telephone Projects

The case study will be no more than 3 pages and must include the total number of PBXs designed and implemented into production on a global scale supporting 450 personnel in one building and demonstrate recent experience (within the past three (3) years immediately prior to the date of solicitation). The total dollar amount shall be provided yearly per project implementation and the Offeror shall provide Network Architecture Diagrams & the SOW with relevant, highlighted sections.

PBX Design and Implementation — artifacts must demonstrate:

1. How the Offeror configured and deployed a scalable PBX on a global scale where sites have different requirements
2. Provide a network diagram
3. Show how the solution was turnkey

Part Two- Past Performance Assessment (CPARS past performance record or Attachment J-8) for each Relevant Experience Project

For each case study, the Offeror must submit the associated past performance assessment. Acceptable forms of past performance assessments are data contained in Contractor Performance Assessment Reporting System (CPARS) or a Past Performance Survey *(Attachment J-8)*.

The Offeror must demonstrate favorable past performance for each project submitted as a case study. The burden of providing thorough, organized and complete past performance information rests with the Offeror. Failure to submit qualifying past contractual performance information when it exists will be deemed a material nonconformity and result in the offer being summarily rejected.

Favorable past performance is defined as: each past performance assessment receiving a satisfactory or better rating for the majority of rated elements. The Offeror will not be evaluated favorably or unfavorably on past performance in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available. Offerors will assume DOS has no past performance records at hand and that no member of DOS has personal knowledge of the Offeror's past performance.

Commercial vs. Federal Past Performance: DOS will consider commercial and federal past performance equally. DOS reserves the right to verify past performance information and may use broad discretion in considering additional past performance sources. DOS retains the right to validate the sources and content of past performance information.

Past Performance (when CPARS information exists): If interim or final ratings exist in CPARS for the submitted project, the Offeror must provide a copy of this rating with their proposal. If a final rating is not available, the most current past performance information will be used.

Past Performance (when CPARS information does not exist): The Offeror may ONLY submit *Attachment J-8,* Past Performance Survey in the event CPARS information is not available. If CPARS information is available for any submitted REP it must be used for the Past Performance evaluation.

If the project(s) are considered Non-U.S. Federal projects; the Offeror must submit a Past Performance Survey using the template in Attachment J-8, "Past Performance Survey." No other format or additional proposal documentation will be considered.

Using the Past Performance Survey in Attachment J-8: the Offeror will provide the survey directly to each of the references. The Past Performance Survey must be completed and signed by a Contracting Officer, or Contracting Officer's Representative, or Contracting Officer's Technical Representative with cognizance over the submitted project. For a commercial project, the Past Performance Rating Form must be completed and signed by a Corporate Officer/Official of the customer with cognizance over the submitted project.

The Offeror will instruct each rater to send a completed form directly back to the Offeror. The Offeror must submit all Past Performance Rating Forms, as applicable, with their proposal submission.

Misleading Information: In the event the evaluation team discovers misleading, falsified, and/or fraudulent past performance ratings, the Offeror will be eliminated from further consideration for award. Falsification of any proposal submission, documents, or statements may subject the Offeror to civil or criminal prosecution under Section 1001 of Title 18 of the United States Code.

Adverse Past Performance Narrative (***Optional one page***): An Offeror may submit a one-page narrative for each project being used for past performance to provide information on problems encountered on the submitted projects and the Offeror's corrective actions. This submission is not required but may be included to address past performance assessments where the majority of rating elements are below satisfactory. The Government will consider this information, as well as information obtained from any other sources, when evaluating the Offeror's past performance.

Pool Two: Factor Three — Secondary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below

- Adhere to prescribed page limits

- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Challenges in this section:

- Technical Security and Safeguards
- Hybrid Work Environment
- Telecommunications Center Power Management
- Data Center Infrastructure Management Integration

- Data Sharing
- Overseas Logistics
- PBX Solution Architecture

Pool Two: Factor Four — Cybersecurity Approach

Part One — Supply Chain Risk Management (4 pages)

The Offeror shall describe its approach to supply chain risk management and, at a minimum, address:

1. Specific practices currently in place to reduce supply chain risk.
2. Actions taken to identify, manage and mitigate supply chain and cybersecurity risk.
3. Approach to mitigating and/or eliminating the risk of sabotage, maliciously introduced unwanted function, or other subversion to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of devices delivered to the Government.
4. The Offeror's intention regarding obtaining CMMC, the target certification level, and a tentative timetable for attaining it.
5. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror, to include ISO certifications (e.g., ISO/IEC 27001:2013, ISO 28000:2007 and ISO 9001:2015).
6. A narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services.
7. Actions taken to mitigate widespread supply chain sabotage when it occurs within the production environment. Describe how to contain and remove the threat while minimizing operational impacts.
8. Approach to managing sourcing risks as an integral part of enterprise architecture planning and design.

Part Two — Cybersecurity History (4 pages)

The Offeror shall describe its cybersecurity history and, at a minimum, address:

1. Number of Cybersecurity violations, infractions, or concerns in the last 5 years. Include date, summary and mitigation. This includes any violations from subcontractors working with or on behalf of.
2. Cybersecurity violations planning. Provide a plan on how the company will address cybersecurity violations, infractions or concerns.
3. Systems Assessed in the last 5 years. Include timelines, summaries, ATO and POA&M status for systems developed or implemented by the vendor in government environments.
4. For any system requiring connection to the Department's infrastructure or requiring access to federal information or data, provide a self-assessment using NIST SP 171 for each system.
5. Positions that would require elevated access to the Department's infrastructure. Provide a summary of the process in which these personnel would be managed, to include any

training provided by the company or expected by the government to provide in order to maintain federal cyber hygiene standards. Additionally provide anything needed by the government to assist with these processes.

6. If planning to develop any technology for the government, provide a plan on how the software and/or hardware will be secured. Include how federal cyber hygiene standards and NIST requirements will be obtained and maintained.

Pool Two: Factor Five — Management Approach

Program Management - 4 pages

The Offeror shall describe its proposed management structure, the position within the overall corporate organization of the division or group proposed to perform this effort, and the level of corporate project oversight planned in terms of authority to make programmatic decisions and implement design solutions. In addition, the Offeror shall provide the resume of the proposed Program Manager (PM). If the proposed PM is not a current employee, then the resume must include a statement that the prospective employee has authorized his/her resume to be submitted, intends to accept employment if the Contractor is selected for award and that the parties have discussed salary parameters. If the PM candidate becomes unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The Offeror shall also describe its management solution including the following topics:

- The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the tasks awarded under this contract.
- The proposed Project Management approach and the Offeror's methodology for ensuring cost, schedule and performance objectives (including service-level agreements or other types of performance metrics and measures) are controlled, reported, and managed.
- The approach for managing multiple task orders for this effort, including:
    - The tools and methodologies for planning the activities of its team(s),
    - Scheduling, organizing, and deploying resources,
    - Controlling of task execution, monitoring progress, status reporting, resolving critical issues, and planning for subsequent phases of work. Earned Value Management.
- The Offeror's proposed Earned Value Management System (EVMS), its level of compliance with ANSI/EIA-748, and its ability to capture and evaluate cost, schedule, risk, and performance data throughout the life of a task.
- The governance and reporting structure and the degree to which it provides transparency and Government access to real time cost, schedule and performance metrics

Quality Control Solution - 2 pages

The Offeror shall describe its Quality Control solution and how it relates to DOS' objectives stated in Section C. The Offeror's Quality Control solution shall include the following information:

- A description of the Quality Control review/audit process, documentation of the process, methods of internal review, participants in the review and the frequency of review.
- A description of the approach and procedures for handling corrective actions.

Recruitment, Retention, and Training- 3 pages

The Offeror shall describe actions it takes to recruit, train, and retain high-quality personnel, including a description of its processes, procedures, and policies.

Of particular interest is the demonstration of an innovative methodology rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract.

Using *Attachment J-5, Staffing Levels Profile Form*, the Offeror shall provide the number of personnel currently in place within the cognizant business unit (i.e., the legal entity proposing on this procurement), the number of personnel with security credentials, the education and professional certifications obtained by the workforce, their average length of service, and the turnover rate experience of the workforce for last three (3) year period. The turnover rate is defined as the number of personnel who departed (regardless of reason) divided by the total number of personnel at the end of the period. *(This matrix is excluded from the page limitations)*

In the summary page provide a count of current employees aligned to current positions held and the duration employed (prime and teaming partners). Each employee shall be referenced in a single position that is currently held by that individual.

Using *Attachment J-6, Labor Category Table*, the Offeror shall describe the personnel qualifications and experience for each of its labor categories, including a crosswalk with the Government's labor categories and the associated education and experience.

Pool Two: Factor Six — Ability to Achieve Results Through Teaming

In 3 pages, the Offeror shall describe its approach to developing relationships with subcontractors and teaming partners, and specifically how it will continually provide DOS with the best sources of solutions and services. The Offeror's response should demonstrate not only a systematic approach to identifying the most relevant and modern technologies, services, and techniques available in the marketplace, but should also discuss their approach to integrating various subcontractors and teaming partners to successfully meet the Department's objectives as described in task order requirements.

L.10.3 Pool Three- Total Small Business Set-Aside

Pool Three: Minimum Criteria (Go/No-Go)

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offeror's not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. **Offerors unable to substantiate meeting all Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed**.

Title of Evaluation Factor	Explanation
Security Clearances	Offerors shall possess, and provide proof of, a valid Top Secret Facility Clearance or higher at the time of proposal submission. Offerors shall certify their ability to submit all key personnel cleared at the Top Secret or Secret level for reciprocity on Day 1 at time of proposal Offerors shall submit their DD254 at time of proposal.
NDAA Compliance	Completed Express NDAA Certification in support of the John S. McCain National Defense Authorization Act Fiscal Year 2019 (Pub. L. 115-232). Paragraph (a)(1)(B) of section 889 in accordance with FAR 52.204-26, Covered Telecommunications Equipment or Services Representation and/or other appropriate documentation that it does not provide covered services or supplies as defined by the NDAA
Certification: Pool Three	Offerors shall be certified at the Proof must be provided with Phase 1 submission. Offerors shall be provide proof of certification with their Phase 1 submission per pool. 1. CMMI Development — Level 3 or higher 2. CMMI Service — Level 3 or higher 3. ISO 9001 certified
Intent/Cover Letter	A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government, including which Pools it intends to bid on. The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least 180 calendar days from the date of receipt by the Government.

Pool Three: Factor One — Primary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below
- Adhere to prescribed page limits
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Pool Three – Primary Technical Challenges
Data Center Modernization
Problem Statement: A large portion of the current Data Center utilize on-premises legacy custom GOTS application supporting the Configuration Management Database (CMDB), Service Requests (SRs), and Security Information and Event Management (SIEM) functions. This application serves as a single front endpoint for operational and business needs, and requires modernization to meet a more dynamic, automated, and cross platform capabilities of today's technology.
Challenge: Develop a strategy to migrate and utilize COTS, Cloud products, and/or design new GOTS system for a CMDB, SR, and SIEM solution. System must integrate with other platforms for data queries and feeds, provide a single front endpoint for use.
Assumptions: DOS is shifting from an on-premises environment to hybrid and to support remote workforce. Solution will be accessible on-premises and portions or all accessible off-premises. On-premises work presence is a hard requirement for classified networks. In addition, ensuring that the solution does not create additional user overhead and inefficacies with multiple front endpoints, and allows flexibility for future business needs is critical.
Format/Instructions: Develop a white paper of no longer than three (3) pages. This must include proposed architectural drawings. Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.

Cloud Security Automation

Problem Statement: DoS operates multiple cloud platforms; IaaS, PaaS, SaaS each with its own platform-specific operational security environment. Each of these platforms has native security tools and built-in capabilities to aid with cyber management and incident detection but requires security engineers and analysts to monitor and respond on each platform individually. As the use of the platforms scale up, the engineers and analysts can't keep up. DoS wants to take advantage of platform native tools and other security tools to augment and automate processes as an enterprise capability, yet not rely on increasing staffing as use scales up.

Challenge: To mature toward a DevSecOps capability, automation must be implemented across the cloud platforms to improve monitoring, security, and risk management at the enterprise level. How will you, the Offeror, approach unifying cyber security management of the numerous cloud platforms, taking into consideration the on-premises components, to improve monitoring and risk management while first preventing and then detecting incidents. Please address this in terms of technical implementation, governance, organization limitations, and team(s) structure. How would the Offeror approach security in a fragmented environment, with several distinct organizations responsible for elements of cyber, sometimes with overlapping responsibilities for the interconnectivity of cloud platforms and on-premises networks?

Assumptions: Most of the current cyber capabilities are focused on legacy on-premises implementation, not adaptable to cloud platforms and aligned with the Department's cloud strategy.

Format/Instructions: Develop a white paper of no longer than three (3) pages. This must include proposed architectural drawings. Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.

Pool Three: Factor Two — Past Experience and Past Performance

Part One- Past Experience Submission

The Offeror must demonstrate relevant experience by submitting two (2) Relevant Experience Projects (REPs) for Cloud and Data Centers. Use the REP Template in accordance with the instructions herein. A REP may consist of a contract or task order issued against an IDIQ or BPA; but simply holding an IDIQ contract or BPA is not sufficient. The Offeror must have performed work on a task order issued against the contract or BPA.

Using REP Template, the Offeror shall identify two recent and relevant Government and/or commercial efforts on which it has performed as the prime contractor.

In a ***one-page addendum attached to each REP***, the Offeror shall:

1. Include a description of how the Offeror's past performance demonstrates their capability and capacity to deliver high quality service and solutions in a performance-based environment.

2. Focus on the key requirements of the project, as well as the size, scope and complexity of the efforts, the relevance to the pool the performance is being submitted for and if applicable, the performance measures and service level metrics applied to specific program objectives, and the actual results achieved against those measures. The service-level agreements or performance standards should be specific and show the target performance levels that are set forth under the applicable contracts.
3. A summary of performance ratings shall be provided showing the performance results achieved by the prospective Offeror for the latest two contract rating periods.

Part Two- Past Performance Assessment (CPARS past performance record or Attachment J-8) for each Relevant Experience Project

For each REP, the Offeror must submit the associated past performance assessment. Acceptable forms of past performance assessments are data contained in Contractor Performance Assessment Reporting System (CPARS) or a Past Performance Survey *(Attachment J-8)*.

The Offeror must demonstrate favorable past performance for each project submitted as a case study. The burden of providing thorough, organized and complete past performance information rests with the Offeror. Failure to submit qualifying past contractual performance information when it exists will be deemed a material nonconformity and result in the offer being summarily rejected.

Favorable past performance is defined as: each past performance assessment receiving a satisfactory or better rating for the majority of rated elements. The Offeror will not be evaluated favorably or unfavorably on past performance in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available. Offerors will assume DOS has no past performance records at hand and that no member of DOS has personal knowledge of the Offeror's past performance.

Commercial vs. Federal Past Performance: DOS will consider commercial and federal past performance equally. DOS reserves the right to verify past performance information and may use broad discretion in considering additional past performance sources. DOS retains the right to validate the sources and content of past performance information.

Past Performance (when CPARS information exists): If interim or final ratings exist in CPARS for the submitted project, the Offeror must provide a copy of this rating with their proposal. If a final rating is not available, the most current past performance information will be used.

Past Performance (when CPARS information does not exist): The Offeror may ONLY submit Attachment J-8, Past Performance Survey in the event CPARS information is not available. If CPARS information is available for any submitted REP it must be used for the Past Performance evaluation.

If the project(s) are considered Non-U.S. Federal projects; the Offeror must submit a Past Performance Survey using the template in Attachment J-8, "Past Performance Survey." No other format or additional proposal documentation will be considered.

Using the Past Performance Survey in Attachment J-8: the Offeror will provide the survey directly to each of the references. The Past Performance Survey must be completed and signed by a Contracting Officer, or Contracting Officer's Representative, or Contracting Officer's Technical Representative with cognizance over the submitted project. For a commercial project, the Past Performance Rating Form must be completed and signed by a Corporate Officer/Official of the customer with cognizance over the submitted project.

The Offeror will instruct each rater to send a completed form directly back to the Offeror. The Offeror must submit all Past Performance Rating Forms, as applicable, with their proposal submission.

Misleading Information: In the event the evaluation team discovers misleading, falsified, and/or fraudulent past performance ratings, the Offeror will be eliminated from further consideration for award. Falsification of any proposal submission, documents, or statements may subject the Offeror to civil or criminal prosecution under Section 1001 of Title 18 of the United States Code.

Adverse Past Performance Narrative ***(Optional one page)***: An Offeror may submit a ***one-page*** narrative for each project being used for past performance to provide information on problems encountered on the submitted projects and the Offeror's corrective actions. This submission is not required but may be included to address past performance assessments where the majority of rating elements are below satisfactory. The Government will consider this information, as well as information obtained from any other sources, when evaluating the Offeror's past performance.

Pool Three: Factor Three — Secondary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below
- Adhere to prescribed page limits
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Technical Challenges in this section include:
Multiple Cloud Platforms
Testing Environment

Pool Three: Factor Four — Cybersecurity Approach

Part One — Supply Chain Risk Management (4 pages)

The Offeror shall describe its approach to supply chain risk management and, at a minimum, address:

1. Specific practices currently in place to reduce supply chain risk.

2. Actions taken to identify, manage and mitigate supply chain and cybersecurity risk.
3. Approach to mitigating and/or eliminating the risk of sabotage, maliciously introduced unwanted function, or other subversion to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of devices delivered to the Government.
4. The Offeror's intention regarding obtaining CMMC, the target certification level, and a tentative timetable for attaining it.
5. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror, to include ISO certifications (e.g., ISO/IEC 27001:2013, ISO 28000:2007 and ISO 9001:2015).
6. A narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services.
7. Actions taken to mitigate widespread supply chain sabotage when it occurs within the production environment. Describe how to contain and remove the threat while minimizing operational impacts.
8. Approach to managing sourcing risks as an integral part of enterprise architecture planning and design.

Part Two — Cybersecurity History (4 pages)

The Offeror shall describe its cybersecurity history and, at a minimum, address:

1. Number of Cybersecurity violations, infractions, or concerns in the last 5 years. Include date, summary and mitigation. This includes any violations from subcontractors working with or on behalf of.
2. Cybersecurity violations planning. Provide a plan on how the company will address cybersecurity violations, infractions or concerns.
3. Systems Assessed in the last 5 years. Include timelines, summaries, ATO and POA&M status for systems developed or implemented by the vendor in government environments.
4. For any system requiring connection to the Department's infrastructure or requiring access to federal information or data, provide a self-assessment using NIST SP 171 for each system.
5. Positions that would require elevated access to the Department's infrastructure. Provide a summary of the process in which these personnel would be managed, to include any training provided by the company or expected by the government to provide in order to maintain federal cyber hygiene standards. Additionally provide anything needed by the government to assist with these processes.
6. If planning to develop any technology for the government, provide a plan on how the software and/or hardware will be secured. Include how federal cyber hygiene standards and NIST requirements will be obtained and maintained.

Part Three — Pool Three-Specific, Security Controls (2 pages, with up to 10 pages of attachments)

Provide information from a past project where you identified and established security controls for a platform (IaaS/PaaS, etc.) that can be inherited. Provide all necessary documentation for those inheritable controls. Describe your approach to managing shared controls. Please provide the narrative in no more than two pages and any attachments in no more than 10 pages for controls.

Pool Three: Factor Five — Management Approach

Program Management - 4 pages

The Offeror shall describe its proposed management structure, the position within the overall corporate organization of the division or group proposed to perform this effort, and the level of corporate project oversight planned in terms of authority to make programmatic decisions and implement design solutions. In addition, the Offeror shall provide the resume of the proposed Program Manager (PM). If the proposed PM is not a current employee, then the resume must include a statement that the prospective employee has authorized his/her resume to be submitted, intends to accept employment if the Contractor is selected for award and that the parties have discussed salary parameters. If the PM candidate becomes unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The Offeror shall also describe its management solution including the following topics:

- The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the tasks awarded under this contract.
- The proposed Project Management approach and the Offeror's methodology for ensuring cost, schedule and performance objectives (including service-level agreements or other types of performance metrics and measures) are controlled, reported, and managed.
- The approach for managing multiple task orders for this effort, including:
- The tools and methodologies for planning the activities of its team(s),
- Scheduling, organizing, and deploying resources,
- Controlling of task execution, monitoring progress, status reporting, resolving critical issues, and planning for subsequent phases of work. Earned Value Management.
- The Offeror's proposed Earned Value Management System (EVMS), its level of compliance with ANSI/EIA-748, and its ability to capture and evaluate cost, schedule, risk, and performance data throughout the life of a task.
- The governance and reporting structure and the degree to which it provides transparency and Government access to real time cost, schedule and performance metrics.

Quality Control Solution - 2 pages

The Offeror shall describe its Quality Control solution and how it relates to DOS' objectives stated in Section C. The Offeror's Quality Control solution shall include the following information:

- A description of the Quality Control review/audit process, documentation of the process, methods of internal review, participants in the review and the frequency of review.
- A description of the approach and procedures for handling corrective actions.

Recruitment, Retention, and Training- 3 pages

The Offeror shall describe actions it takes to recruit, train, and retain high-quality personnel, including a description of its processes, procedures, and policies.

Of particular interest is the demonstration of an innovative methodology rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract.

Using *Attachment J-5, Staffing Levels Profile Form*, the Offeror shall provide the number of personnel currently in place within the cognizant business unit (i.e., the legal entity proposing on this procurement), the number of personnel with security credentials, the education and professional certifications obtained by the workforce, their average length of service, and the turnover rate experience of the workforce for last three (3) year period. The turnover rate is defined as the number of personnel who departed (regardless of reason) divided by the total number of personnel at the end of the period. *(This matrix is excluded from the page limitations)*

In the summary page provide a count of current employees aligned to current positions held and the duration employed (prime and teaming partners). Each employee shall be referenced in a single position that is currently held by that individual.

Using *Attachment J-6, Labor Category Table*, the Offeror shall describe the personnel qualifications and experience for each of its labor categories, including a crosswalk with the Government's labor categories and the associated education and experience.

Pool Three: Factor Six — Ability to Achieve Results Through Teaming

In 3 pages, the Offeror shall describe its approach to developing relationships with subcontractors and teaming partners, and specifically how it will continually provide DOS with the best sources of solutions and services. The Offeror's response should demonstrate not only a systematic approach to identifying the most relevant and modern technologies, services, and techniques available in the marketplace, but should also discuss their approach to integrating various subcontractors and teaming partners to successfully meet the Department's objectives as described in task order requirements.

L.10.4 Pool Four- Full and Open Competition

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offeror's not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. **Offerors unable to substantiate meeting all Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed**.

	Instructions to Offerors
Security Clearances	Offerors shall possess, and provide proof of, a valid TOP SECRET Facility Clearance or higher at the time of proposal submission. Offerors shall certify their ability to submit all key personnel cleared at the Top Secret or Secret level for reciprocity on Day 1 at time of proposal Offerors shall submit their DD254 at time of proposal.
FEDRAMP	Provide your FedRAMP certification of a product developed by your company OR Provide an example of a COTs product/SaaS that your company has Developed and/or a SaaS/cloud product that your company was responsible for taking through the Risk Management Framework process in order to obtain FedRAMP Certification or Agency ATO — E.g., Provide an FedRAMP or ATO letter or link to the FedRAMP site
NDAA Compliance	Completed Express NDAA Certification in support of the John S. McCain National Defense Authorization Act Fiscal Year 2019 (Pub. L. 115-232). Paragraph (a)(1)(B) of section 889 in accordance with FAR 52.204-26, Covered Telecommunications Equipment or Services Representation and/or other appropriate documentation that it does not provide covered services or supplies as defined by the NDAA
Certifications Pool Four	Offerors shall be certified at the Proof must be provided with Phase 1 submission. Offerors shall be provide proof of certification with their Phase 1 submission per pool. 1. ISO 27001 certification
Intent/Cover Letter	A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government, including which Pools it intends to bid on.

	The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least 180 calendar days from the date of receipt by the Government.
Small Business Subcontracting Plan	

Pool Four: Factor One — Primary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below
- Adhere to prescribed page limits
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Pool Four – Primary Technical Challenge
Replacing Legacy Systems **Problem Statement:** As more modern technological solutions come to the forefront the need to replace legacy systems are on the rise in an effort for organizations to stay current with modern technology. More organizations are choosing to migrate their legacy systems to the cloud for various reasons including its benefits such as mobility, increased collaboration among dispersed teams and systems, disaster recovery, scalability, and security. Although there are many benefits to migrating to the cloud, often organizations are faced with many challenges that are not always predictable and are faced with addressing these issues before, during and sometimes after the migration. **Challenge:** Provide an example of a legacy system that the Offeror has migrated to the cloud and share the Offeror's approach as well as some of the challenges the Offeror faced and how the Offeror overcame them. What type of legacy systems have you migrated? How many users were on the legacy system? How were they affected during the migration? What was the communication plan to those users for a smooth transition? Was the legacy system to be migrated originally on-premises or was it already a cloud-based system? What were the challenges faced before, during, and after the migration? How did the Offeror overcome the identified challenges? What were the benefits of moving the legacy system to the cloud? How long did the process take? What type of tools were used to complete the migration?

Assumptions: The company has experience migrating a legacy system to the cloud or is in the process of migrating a legacy system and has extensive knowledge of an approach to successfully complete the task.

Format/Instructions: Develop a white paper of no longer than three (3) pages. Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.

Pool Four: Factor Two — Past Experience and Past Performance

Part One- Past Experience Submission

The Offeror must demonstrate relevant experience by submitting two (2) Relevant Experience Projects (REPs). Use the REP Template in accordance with the instructions herein. A REP may consist of a contract or task order issued against an IDIQ or BPA; but simply holding an IDIQ contract or BPA is not sufficient. The Offeror must have performed work on a task order issued against the contract or BPA.

Using Relevant Past Experience Template, the Offeror, shall identify two recent and relevant Government and/or commercial efforts on which it has performed as the prime contractor.

In a ***5 page*** addendum to the REP Template the Offeror shall:

1. Describe how the Offeror's past performance demonstrates their capability and capacity to deliver high quality service and solutions in a performance-based environment.
2. Focus on the key requirements of the project, as well as the size, scope and complexity of the efforts, the relevance to the pool the performance is being submitted for and if applicable, the performance measures and service level metrics applied to specific program objectives, and the actual results achieved against those measures. The service-level agreements or performance standards should be specific and show the target performance levels that are set forth under the applicable contracts.

In the addendum, the Offeror shall explain if the submission includes the following experience:

1. Building an enterprise-wide application(s)
2. Examples of no code/low code application(s)
3. Any legacy applications migrated from on premise to the cloud
4. Show how the team used modern programming languages to implement the solution
5. Show how the team enforced quality assurance during and after deployment
6. Show how the application added value to the organization
7. Show how efficient the team was with completing development within the given time frame with minimal scope creep
8. Share the chosen development life cycle and share how this contributed to the project's success
9. Show/Explain how the solution (i.e., Your past experience) saved the organization in time and money.
10. Show/Explain how well the new application was adopted and/or used compared to the legacy application.

11. Show/Explain how your company reduced the risks for the government agency when migrating applications
12. Show/Explain how you created agnostic components for your application framework. (i.e., how easy was it to scale and/or build upon)
13. Show how your solution improved operations and maintenance overtime and which of the following types of maintenance were considered Corrective, Preventative, Perfective, and Adaptive.

Part Two- Past Performance Assessment (CPARS past performance record or Attachment J-8) for each Relevant Experience Project

For each REP, the Offeror must submit the associated past performance assessment. Acceptable forms of past performance assessments are data contained in Contractor Performance Assessment Reporting System (CPARS) or a Past Performance Survey *(Attachment J-8)*.

The Offeror must demonstrate favorable past performance for each REP. The burden of providing thorough, organized and complete past performance information rests with the Offeror. Failure to submit qualifying past contractual performance information when it exists will be deemed a material nonconformity and result in the offer being summarily rejected.

Favorable past performance is defined as: each past performance assessment receiving a satisfactory or better rating for the majority of rated elements. The Offeror will not be evaluated favorably or unfavorably on past performance in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available. Offerors will assume DOS has no past performance records at hand and that no member of DOS has personal knowledge of the Offeror's past performance.

Commercial vs. Federal Past Performance: DOS will consider commercial and federal past performance equally. DOS reserves the right to verify past performance information and may use broad discretion in considering additional past performance sources. DOS retains the right to validate the sources and content of past performance information.

Past Performance (when CPARS information exists): If interim or final ratings exist in CPARS for the submitted project, the Offeror must provide a copy of this rating with their proposal. If a final rating is not available, the most current past performance information will be used.

Past Performance (when CPARS information does not exist): The Offeror may ONLY submit Attachment J-8, Past Performance Survey in the event CPARS information is not available. If CPARS information is available for any submitted REP it must be used for the Past Performance evaluation.

If the project(s) are considered Non-U.S. Federal projects; the Offeror must submit a Past Performance Survey using the template in Attachment J-8, "Past Performance Survey." No other format or additional proposal documentation will be considered.

Using the Past Performance Survey in Attachment J-8: the Offeror will provide the survey directly to each of the references. The Past Performance Survey must be completed and signed by a

Contracting Officer, or Contracting Officer's Representative, or Contracting Officer's Technical Representative with cognizance over the submitted project. For a commercial project, the Past Performance Rating Form must be completed and signed by a Corporate Officer/Official of the customer with cognizance over the submitted project.

The Offeror will instruct each rater to send a completed form directly back to the Offeror. The Offeror must submit all Past Performance Rating Forms, as applicable, with their proposal submission.

Misleading Information: In the event the evaluation team discovers misleading, falsified, and/or fraudulent past performance ratings, the Offeror will be eliminated from further consideration for award. Falsification of any proposal submission, documents, or statements may subject the Offeror to civil or criminal prosecution under Section 1001 of Title 18 of the United States Code.

Adverse Past Performance Narrative (***Optional one page***): An Offeror may submit a one-page narrative for each project being used for past performance to provide information on problems encountered on the submitted projects and the Offeror's corrective actions. This submission is not required but may be included to address past performance assessments where the majority of rating elements are below satisfactory. The Government will consider this information, as well as information obtained from any other sources, when evaluating the Offeror's past performance.

Pool Four: Factor Three — Secondary Technical Challenges

Offerors shall:

Submit written responses in pdf format to the technical challenges identified in the table below

Adhere to prescribed page limits

Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Challenges in this section:

- Public Facing Web Applications
- COTS Product
- Mobile Application

Pool Four: Factor Four — Cybersecurity Approach

Part One — Supply Chain Risk Management (4 pages)

The Offeror shall describe its approach to supply chain risk management and, at a minimum, address:

1. Specific practices currently in place to reduce supply chain risk.
2. Actions taken to identify, manage and mitigate supply chain and cybersecurity risk.

3. Approach to mitigating and/or eliminating the risk of sabotage, maliciously introduced unwanted function, or other subversion to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of devices delivered to the Government.
4. The Offeror's intention regarding obtaining CMMC, the target certification level, and a tentative timetable for attaining it.
5. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror, to include ISO certifications (e.g., ISO/IEC 27001:2013, ISO 28000:2007 and ISO 9001:2015).
6. A narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services.
7. Actions taken to mitigate widespread supply chain sabotage when it occurs within the production environment. Describe how to contain and remove the threat while minimizing operational impacts.
8. Approach to managing sourcing risks as an integral part of enterprise architecture planning and design.

Part Two — Cybersecurity History (4 pages)

The Offeror shall describe its cybersecurity history and, at a minimum, address:

1. Number of Cybersecurity violations, infractions, or concerns in the last 5 years. Include date, summary and mitigation. This includes any violations from subcontractors working with or on behalf of.
2. Cybersecurity violations planning. Provide a plan on how the company will address cybersecurity violations, infractions or concerns.
3. Systems Assessed in the last 5 years. Include timelines, summaries, ATO and POA&M status for systems developed or implemented by the vendor in government environments.
4. For any system requiring connection to the Department's infrastructure or requiring access to federal information or data, provide a self-assessment using NIST SP 171 for each system.
5. Positions that would require elevated access to the Department's infrastructure. Provide a summary of the process in which these personnel would be managed, to include any training provided by the company or expected by the government to provide in order to maintain federal cyber hygiene standards. Additionally provide anything needed by the government to assist with these processes.
6. If planning to develop any technology for the government, provide a plan on how the software and/or hardware will be secured. Include how federal cyber hygiene standards and NIST requirements will be obtained and maintained.

Part Three — Pool Four-Specific, DevSecOps - 4 pages

Provide information from a past project during which the Offeror facilitated the ATO process for an application. Offerors shall describe:

1. How they integrated the DevSecOps concept into the Application Development and Agile process.
2. How security was integrated into the Application Development process
3. How is testing was conducted
4. What type of authentication was used
5. The type of code was used
6. Was the code Open Source
7. How did the application address the top Common Weakness Enumeration with respect to software developed
8. What security testing tools and application shielding products were used
9. What was the process to manage patch management and code updates/upgrades
10. How is data protected?
11. How is RBAC used at the application level

Pool Four: Factor Five — Management Approach

Program Management - 4 pages

The Offeror shall describe its proposed management structure, the position within the overall corporate organization of the division or group proposed to perform this effort, and the level of corporate project oversight planned in terms of authority to make programmatic decisions and

implement design solutions. In addition, the Offeror shall provide the resume of the proposed Program Manager (PM). If the proposed PM is not a current employee, then the resume must include a statement that the prospective employee has authorized his/her resume to be submitted, intends to accept employment if the Contractor is selected for award and that the parties have discussed salary parameters. If the PM candidate becomes unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The Offeror shall also describe its management solution including the following topics:

- The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the tasks awarded under this contract.
- The proposed Project Management approach and the Offeror's methodology for ensuring cost, schedule and performance objectives (including service-level agreements or other types of performance metrics and measures) are controlled, reported, and managed.
- The approach for managing multiple task orders for this effort, including:
    - The tools and methodologies for planning the activities of its team(s),
    - Scheduling, organizing, and deploying resources,
    - Controlling of task execution, monitoring progress, status reporting, resolving critical issues, and planning for subsequent phases of work. Earned Value Management.
- The Offeror's proposed Earned Value Management System (EVMS), its level of compliance with ANSI/EIA-748, and its ability to capture and evaluate cost, schedule, risk, and performance data throughout the life of a task.

- The governance and reporting structure and the degree to which it provides transparency and Government access to real time cost, schedule and performance metrics

Quality Control Solution - 2 pages

The Offeror shall describe its Quality Control solution and how it relates to DOS' objectives stated in Section C. The Offeror's Quality Control solution shall include the following information:

- A description of the Quality Control review/audit process, documentation of the process, methods of internal review, participants in the review and the frequency of review.
- A description of the approach and procedures for handling corrective actions.

Recruitment, Retention, and Training- 3 pages

The Offeror shall describe actions it takes to recruit, train, and retain high-quality personnel, including a description of its processes, procedures, and policies.

Of particular interest is the demonstration of an innovative methodology rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract.

Using *Attachment J-5, Staffing Levels Profile Form*, the Offeror shall provide the number of personnel currently in place within the cognizant business unit (i.e., the legal entity proposing on this procurement), the number of personnel with security credentials, the education and professional certifications obtained by the workforce, their average length of service, and the turnover rate experience of the workforce for last three (3) year period. The turnover rate is defined as the number of personnel who departed (regardless of reason) divided by the total number of personnel at the end of the period. *(This matrix is excluded from the page limitations)*

In the summary page provide a count of current employees aligned to current positions held and the duration employed (prime and teaming partners). Each employee shall be referenced in a single position that is currently held by that individual.

Using *Attachment J-6, Labor Category Table*, the Offeror shall describe the personnel qualifications and experience for each of its labor categories, including a crosswalk with the Government's labor categories and the associated education and experience.

Pool Four: Factor Six — Ability to Achieve Results Through Teaming

In 3 pages, the Offeror shall describe its approach to developing relationships with subcontractors and teaming partners, and specifically how it will continually provide DOS with the best sources of solutions and services. The Offeror's response should demonstrate not only a systematic approach to identifying the most relevant and modern technologies, services, and techniques available in the marketplace, but should also discuss their approach to integrating various subcontractors and teaming partners to successfully meet the Department's objectives as described in task order requirements.

L.10.5 Pool Five- Full and Open Competition

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offeror's not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. **Offerors unable to substantially meet all Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed**.

Title of Evaluation Factor	Language
Security Clearances	Offerors shall possess, and provide proof of, a valid Top Secret Facility Clearance or higher at the time of proposal submission. Offerors shall certify their ability to submit all key personnel cleared at the Top Secret or Secret level for reciprocity on Day 1 at time of proposal Offerors shall submit their DD254 at time of proposal.
NDAA Compliance	Completed Express NDAA Certification in support of the John S. McCain National Defense Authorization Act Fiscal Year 2019 (Pub. L. 115-232). Paragraph (a)(1)(B) of section 889 in accordance with FAR 52.204-26, Covered Telecommunications Equipment or Services Representation and/or other appropriate documentation that it does not provide covered services or supplies as defined by the NDAA
Certifications: Pool Five	Offerors shall be certified at the Proof must be provided with Phase 1 submission. Offerors shall provide proof of certification with their Phase 1 submission per pool. 1. CMMI Service — Level 3 or higher 2. ISO 9001 certified 3. ISO 20000 certified 4. ISO 27000 certified

Intent/Cover Letter	A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government, including which Pools it intends to bid on. The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least 180 calendar days from the date of receipt by the Government.
Small Business Subcontracting Plan	

Pool Five: Factor One — Primary Technical Challenges

Offerors shall:

- Submit written responses in pdf format to the technical challenges identified in the table below
- Adhere to prescribed page limits
- Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Pool Five – Primary Technical Challenge
Remote Working **Problem Statement:** The Department has many locations located not only in the National Capital Region but also throughout the United States. The Department also has many staff working remotely and will also introduce a remote support model to posts abroad. **Challenge:** Describe how you would provide innovative solutions to serve disparate customer locations to include working from home and field offices while reducing contract FTE footprint/office space while simultaneously increasing customer satisfaction and other quality measurements with the same level of service regardless of customer location e.g., work from home, large customer office, field offices. **Assumptions:** Any technology that is part of this approach is approved for use on DOS networks, Offerors will have thought full approach to implementation and a simple technical solution alone is not adequate. Both customers and contract FTE staff examples must be addressed e.g., disparate customers and disparate contractor FTE support staff that service those customers.

Format/Instructions: Create a white paper, no more than four (4) pages in length; Offerors may include an appendix of no more than two (2) pages of graphs, diagrams, etc.
The paper must describe actual experience used and not hypothetical processes. The Offeror is to provide specific examples with KPIs and outcomes.

Pool Five: Factor Two — Past Experience and Past Performance

Part One — Past Experience Submission

Offerors shall read each of the following scenarios and follow the instructions for developing a case study relevant to each scenario to demonstrate recent experience. Offerors shall submit up to two (i.e., no less than one but no more than two) case studies for evaluation by the Government for each scenario.

Scenario 1: Reduction in disruptions as a result of IT process improvements:

Each case study will be 3 pages (not counting relevant artifacts) and must include the total size of the tier one support that must be equivalent in size and scope to DOS' tier one support. It must demonstrate recent experience (within the past three (3) years immediately prior to the date of solicitation). Artifacts must be relevant contract documents or contract deliverables that are clearly highlighted and annotated to support the claims made in the case study.

The case study and artifacts must demonstrate how the Offeror:
(1) managed change
(2) optimized risk exposure while reducing the severity of impact and disruption to end users; and
(3) achieved process improvement implementation success at first attempt. When addressing the above components, it is expected that the Offeror will, at a minimum, address its end user communication program, knowledge transfer approach, and any pertinent roles and responsibilities of the Offeror and the end user
(4) robustness of the end user change management plan including collaboration with the Government on effectively implementing the change
(5) effective risk reporting and management including the discussion of cadences to review risks, issues and the implementation of mitigating actions to address risks and issues
(6) track record of achieving IT process improvements (with examples of such improvements that are relevant to the scope of work in this solicitation) with minimal disruptions to the end user

Scenario 2: ITIL 4

Each case study will be 3-4 pages (not counting relevant artifacts) and must include the total size of the contract submitted for ITIL 4 support that must be equivalent in size and scope to DOS' tier one support. It must demonstrate recent experience (within the past three (3) years immediately prior to the date of solicitation). Artifacts must be relevant contract documents or contract deliverables that are clearly highlighted and annotated to support the claims made in the case study.

The case study and artifacts must demonstrate:

(1) how the Offeror rolled out ITIL 4 training and certification to its service delivery associates
(2) how ITIL 4 is transforming the Offeror's IT service delivery model to be more agile-centric and outcomes-driven to drive business value to its customer
(3) how the Offeror matured status quo ITIL processes and practices on a client contract (corporate internal experience shall not count) specifically the adhering to updated ITIL 4 framework.
(3) the number of individuals that will be ITIL 4 certified relative to the requirements of the scope of work;
(4) transformational examples of when ITIL 4 methodology was introduced
(5) the percent of associates were ITIL 4 certified during the base year of the project
(6) the timeline to certify additional associates in ITIL 4 methodology throughout the life of the project

Scenario 3: Positive User Experience (UX) when interacting with Tier 3 support

Each case study will be 3 pages (not counting relevant artifacts) and must include the total size of the tier three support that must be equivalent in size and scope to DOS' tier three support. It must demonstrate recent experience (within the past three (3) years immediately prior to the date of solicitation). Artifacts must be relevant contract documents or contract deliverables that are clearly highlighted and annotated to support the claims made in the case study.

The case study and artifacts must demonstrate:

(1) Reference to a mechanism to measure end-user satisfaction
(2) References to an achievement of a specific satisfaction measure
(3) An explanation of a methodology to determine continuous improvement of service delivery based on industry frameworks and feedback from the Offeror's clients
(4) A description of a proactive incident management approach
(5) Incident escalation and resolution procedure
(6) Clear escalation paths from Tiers 1 and 2 support and management approach to Tier 3 support
(7) Demonstration of a clear end-to-end ownership of all incidents and management of all service requests, including logging, tracking, resolution and reporting in an IT Service Management (ITSM) platform
(8) Documentation of Tier 3 support approach in a standards and operations procedures manual(s)
(9) Incident response

Scenario Four: ICT Technical Services

Each case study will be no more than 3 pages and must include the total number of products designed and demonstrate recent experience providing ICT technical services, secure technology, non-destructive testing, hardware forensics and signal analysis (within the past three (3) years immediately prior to the date of solicitation). The total dollar amount shall be provided yearly per

project implementation and the Offeror shall provide Network Architecture Diagrams & the SOW with relevant, highlighted sections.

ICT Technical Services — artifacts must demonstrate:

1. Support for the DOS or other Government (e.g., IC) agencies in providing ICT technical services, secure technology, non-destructive testing, hardware forensics and signal analysis, and developing technical reports.

2. How the Offeror innovated processes that would reduce the current equipment processing cycle from 45 days to 30 days.

3. How the Offeror provided creative or alternative best business practices or strategies that optimizes productivity, workmanship, and scalability of future requirements.

4. The Offerors experience and approach for the ICT equipment life cycle management, drafting Standard Operating Procedure (SOP) and performing customer satisfaction survey.

5. The Offerors experience in drafting comprehensive budget plan, monthly labor burn rate reports and budget plan, monthly labor burn rate reports and budget forecasting. Describe your years of experience with classified ICT signal emanation analysis, TEMPEST.

6. The Offerors experience testing and maintaining a certified TEMPEST technical authority/SME.

7. The Offerors experience with systems safeguard anti-tampering products, protective technologies, and safeguarding ICT equipment physical structure.

8. The Offerors experience with OCONUS forward deployment of SMEs in strategic locations to support Post and the regional missions with ICT equipment and the Classified Equipment Lifecycle Management (CELM) program needs

Part Two — Past Performance Assessment (CPARS past performance record or Attachment J-8) for each Relevant Experience Project

For each case study, the Offeror must submit the associated past performance assessment. Acceptable forms of past performance assessments are data contained in Contractor Performance Assessment Reporting System (CPARS) or a Past Performance Survey *(Attachment J-8).*

The Offeror must demonstrate favorable past performance for each project submitted as a case study. The burden of providing thorough, organized and complete past performance information

rests with the Offeror. Failure to submit qualifying past contractual performance information when it exists will be deemed a material nonconformity and result in the offer being summarily rejected.

Favorable past performance is defined as: each past performance assessment receiving a satisfactory or better rating for the majority of rated elements. The Offeror will not be evaluated favorably or unfavorably on past performance in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available. Offerors will assume DOS has no past performance records at hand and that no member of DOS has personal knowledge of the Offeror's past performance.

Commercial vs. Federal Past Performance: DOS will consider commercial and federal past performance equally. DOS reserves the right to verify past performance information and may use broad discretion in considering additional past performance sources. DOS retains the right to validate the sources and content of past performance information.

Past Performance (when CPARS information exists): If interim or final ratings exist in CPARS for the submitted project, the Offeror must provide a copy of this rating with their proposal. If a final rating is not available, the most current past performance information will be used.

Past Performance (when CPARS information does not exist): The Offeror may ONLY submit Attachment J-8, Past Performance Survey in the event CPARS information is not available. If CPARS information is available for any submitted REP it must be used for the Past Performance evaluation.

If the project(s) are considered Non-U.S. Federal projects; the Offeror must submit a Past Performance Survey using the template in Attachment J-8, "Past Performance Survey." No other format or additional proposal documentation will be considered.

Using the Past Performance Survey in Attachment J-8: the Offeror will provide the survey directly to each of the references. The Past Performance Survey must be completed and signed by a Contracting Officer, or Contracting Officer's Representative, or Contracting Officer's Technical Representative with cognizance over the submitted project. For a commercial project, the Past Performance Rating Form must be completed and signed by a Corporate Officer/Official of the customer with cognizance over the submitted project.

The Offeror will instruct each rater to send a completed form directly back to the Offeror. The Offeror must submit all Past Performance Rating Forms, as applicable, with their proposal submission.

Misleading Information: In the event the evaluation team discovers misleading, falsified, and/or fraudulent past performance ratings, the Offeror will be eliminated from further consideration for award. Falsification of any proposal submission, documents, or statements may subject the Offeror to civil or criminal prosecution under Section 1001 of Title 18 of the United States Code.

Adverse Past Performance Narrative (Optional): An Offeror may submit a one-page narrative for each project being used for past performance to provide information on problems encountered on the submitted projects and the Offeror's corrective actions. This submission is not required but

may be included to address past performance assessments where the majority of rating elements are below satisfactory. The Government will consider this information, as well as information obtained from any other sources, when evaluating the Offeror's past performance.

Pool Five: Factor Three — Secondary Technical Challenges

Offerors shall:

Submit written responses in pdf format to the technical challenges identified in the table below

Adhere to prescribed page limits

Submit all artifacts, unless otherwise stated, in pdf format with relevant notes providing attribution back to the technical challenge written response

Technical Challenges include:

Service Transition

Pricing Models

Pool Five: Factor Four — Cybersecurity Approach

Part One-Supply Chain Risk Management (4 pages)

The Offeror shall describe its approach to supply chain risk management and at minimum address:

1. Specific practices currently in place to reduce supply chain risk.
2. Actions taken to identify, manage and mitigate supply chain and cybersecurity risk.
3. Approach to mitigating and/or eliminating the risk of sabotage, maliciously introduced unwanted function, or other subversion to the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of devices delivered to the Government.
4. The Offeror's intention regarding obtaining CMMC, the target certification level, and a tentative timetable for attaining it.
5. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror, to include ISO certifications (e.g., ISO/IEC 27001:2013, ISO 28000:2007 and ISO 9001:2015).
6. A narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services.
7. Actions taken to mitigate widespread supply chain sabotage when it occurs within the production environment. Describe how to contain and remove the threat while minimizing operational impacts.

8. Approach to managing sourcing risks as an integral part of enterprise architecture planning and design.

Part Two – Cybersecurity History (4 pages)

1. Number of Cybersecurity violations, infractions or concerns in the last 5 years. Include date, brief summary and mitigation. This includes any violations from subcontractors working with or on behalf of.
2. Cybersecurity violations planning. Provide a plan on how the company will address cybersecurity violations, infractions or concerns.
3. Systems Assessed in the last 5 years. Include timelines, summaries, ATO and POA&M status for systems developed or implemented by the vendor in government environments.
4. For any system requiring connection to the Department's infrastructure or requiring access to federal information or data, provide a self-assessment using NIST SP 171 for each system.
5. Positions that would require elevated access to the Department's infrastructure. Provide a summary of the process in which these personnel would be managed, to include any training provided by the company or expected by the government to provide in order to maintain federal cyber hygiene standards. Additionally provide anything needed by the government to assist with these processes.
6. If planning to develop any technology for the government, provide a plan on how the software and/or hardware will secured. Include how federal cyber hygiene standards and NIST requirements will be obtained and maintained.

Part Three- Pool Five Specific (2 pages)

The Offeror shall describe its approach in performing Hardware Forensics Analysis (HFA). The Offeror shall describe its approach in collaboration with other Government agencies in maintaining abreast of supply chain risks, product quality, procurement and supplier proliferation in securing the supply chain.

Pool Five: Factor Five — Management Approach

Program Management - 4 pages

The Offeror shall describe its proposed management structure, the position within the overall corporate organization of the division or group proposed to perform this effort, and the level of corporate project oversight planned in terms of authority to make programmatic decisions and implement design solutions. In addition, the Offeror shall provide the resume of the proposed Program Manager (PM). If the proposed PM is not a current employee, then the resume must include a statement that the prospective employee has authorized his/her resume to be submitted, intends to accept employment if the Contractor is selected for award and that the parties have discussed salary parameters. If the PM candidate becomes unavailable at any point during the

evaluation process, the Offeror shall immediately notify the Contracting Officer. The Offeror shall also describe its management solution including the following topics:

- The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the tasks awarded under this contract.
- The proposed Project Management approach and the Offeror's methodology for ensuring cost, schedule and performance objectives (including service-level agreements or other types of performance metrics and measures) are controlled, reported, and managed.
- The approach for managing multiple task orders for this effort, including:
    - The tools and methodologies for planning the activities of its team(s),
    - Scheduling, organizing, and deploying resources,
    - Controlling of task execution, monitoring progress, status reporting, resolving critical issues, and planning for subsequent phases of work. Earned Value Management.
- The Offeror's proposed Earned Value Management System (EVMS), its level of compliance with ANSI/EIA-748, and its ability to capture and evaluate cost, schedule, risk, and performance data throughout the life of a task.
- The governance and reporting structure and the degree to which it provides transparency and Government access to real time cost, schedule and performance metrics

Quality Control Solution - 2 pages

The Offeror shall describe its Quality Control solution and how it relates to DOS' objectives stated in Section C. The Offeror's Quality Control solution shall include the following information:

- A description of the Quality Control review/audit process, documentation of the process, methods of internal review, participants in the review and the frequency of review.
- A description of the approach and procedures for handling corrective actions.

Recruitment, Retention, and Training- 3 pages

The Offeror shall describe actions it takes to recruit, train, and retain high-quality personnel, including a description of its processes, procedures, and policies.

Of particular interest is the demonstration of an innovative methodology rather than basic details of compensation and benefits. Such aspects may include, but are not limited to, training and other skills development programs, opportunities for promotion, awards and recognition or other incentive plans designed to promote high quality performance and employee retention and satisfaction for this contract.

Using *Attachment J-5, Staffing Levels Profile Form*, the Offeror shall provide the number of personnel currently in place within the cognizant business unit (i.e., the legal entity proposing on this procurement), the number of personnel with security credentials, the education and professional certifications obtained by the workforce, their average length of service, and the turnover rate experience of the workforce for last three (3) year period. The turnover rate is defined as the number of personnel who departed (regardless of reason) divided by the total number of personnel at the end of the period. *(This matrix is excluded from the page limitations)*

In the summary page provide a count of current employees aligned to current positions held and the duration employed (prime and teaming partners). Each employee shall be referenced in a single position that is currently held by that individual.

Using *Attachment J-6, Labor Category Table*, the Offeror shall describe the personnel qualifications and experience for each of its labor categories, including a crosswalk with the Government's labor categories and the associated education and experience.

Pool Five: Factor Six — Ability to Achieve Results Through Teaming

In 3 pages, the Offeror shall describe its approach to developing relationships with subcontractors and teaming partners, and specifically how it will continually provide DOS with the best sources of solutions and services. The Offeror's response should demonstrate not only a systematic approach to identifying the most relevant and modern technologies, services, and techniques available in the marketplace, but should also discuss their approach to integrating various subcontractors and teaming partners to successfully meet the Department's objectives as described in task order requirements.

L.11 Content of Resulting Contract

Any contract awarded as a result of this solicitation will contain Part I - The Schedule, Part II - Contract Clauses, and Part III - List of Documents, Exhibits and Other Attachments. Part IV - Section K - Representations, Certifications, and Other Statements of Offerors, will be incorporated into the resulting contract by reference. Blank areas appearing in these sections are to be completed by the Offeror or will be filled in by the Contracting Officer after negotiations have been completed.

L.12 Alternate Proposals

Alternate proposals will not be considered.

(End of Section L)

SECTION M – EVALUATION FACTORS FOR AWARD

M.1 General

(a) The Government is conducting this source selection in accordance with the competitive negotiation source selection procedures contained in FAR Part 15.

(b) In accordance with FAR 52.215-1(f) the Government intends to award multiple contracts with awards made to the responsible offerors whose proposals represents the best value. Best value is defined in FAR Part 2, as the expected outcome of an acquisition that, in the Government's estimation, provides the greatest overall benefit in response to the requirement. The Government will conduct the best value analysis using the factors listed in Section M.3. In performing its best value analysis, the Government will compare any relevant differences among the evaluated proposals to determine which proposal(s) offer(s) the overall best value. This effort will include comparing the strengths, weaknesses and risks associated with each offer.

(c) The Government intends to evaluate proposals and award contracts without discussions with the Offerors except clarifications as described in FAR 15.306(a) and will evaluate each offer on the basis of the Offeror's initial proposal. Therefore, the initial proposal should contain the Offerors' best terms from a technical and cost/price standpoint.

(d) When conducting the evaluation, the Government may use data included by Offerors in their proposals, as well as data obtained from other sources. Each Offeror is responsible for ensuring that the information provided is thorough, accurate, and complete.

M.2 Basis for Award

The Government will award contracts to the responsible Offerors whose proposals are the most advantageous to the Government, price and other factors considered. The Government is conducting five separate and distinct source selections under this solicitation.

The procurement schedule and award decisions on one track will not affect the other track unless a contractor is deemed eligible for award on more than two pools for pools 2-5 or they are deemed eligible for award under pool one and are therefore disqualified from receiving an award on pools 2-5.

There will be five award tracks one for each pool. The Government intends to make multiple contract awards under both tracks. A sufficient number of awards will be made in each Pool to ensure adequate competition at the TO level. Offerors proposing on multiple Pools are advised that award may be made on one, all or any combination of those Pools proposed.

M.3 Evaluation Factors

The selection decision will be based on the following factors:

(a) Go/No-Go (Mandatory Minimum Requirements)

Each proposal review will begin with an initial Go/No-Go screening to determine whether the Offeror fulfills certain required qualifications. Offerors not meeting these Go/No-Go criteria will not receive further consideration and their Stage I response will not be reviewed. Offerors unable to substantiate meeting all Go/No-Go criteria will not receive further consideration and their Phase 1 response will not be reviewed.

(b) Phase One-Non-Price Factors

Factor 1: Technical Challenge
Factor 2: Past Performance and Past Experience

(c) Phase Two- Non-Price Factors
Factor 3: Secondary Technical Challenges
Factor 4: Cybersecurity
Factor 5: Management Approach
Factor 6: Ability to Achieve Results through Teaming

(d) Price Factor: Price

Order of Importance: Non-Price Factors 1 through 6 are listed in descending order of importance. The non-price factors, when combined, are significantly more important than the price factor.

M.3.0 Proposal Preparation Compliance Determination

The Government will review proposals submitted to determine compliance with the proposal preparation instructions. If it is determined that the proposal is substantially not in compliance with the instructions in Section L, the Government may deem that proposal to be unacceptable and it will not be evaluated further. The proposal may be removed from consideration for contract award.

M.3.1 Factor 1: Primary Technical Challenges

In its evaluation, the Government will consider the benefits and risks associated with the Offeror's proposal to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the requirements of the solicitation. The Offeror's response will be evaluated holistically using the total confidence methodology,

M.3.2 Factor 2: Past Performance and Past Experience

The Government will assess its level of Confidence that the Prime Vendor will successfully perform the requirements based on the past experience and past performance.

ADVISORY DOWNSELECT

M.3.3 Factor 3: Secondary Technical Challenges

In its evaluation, the Government will consider the benefits and risks associated with the Offeror's proposal to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the requirements of the solicitation. The Offeror's response will be evaluated holistically using the total confidence methodology

M.3.4 Factor 4: Cybersecurity Approach

In its evaluation, the Government will consider the benefits and risks associated with the Offeror's proposal to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the requirements of the solicitation and assisting DOS in increasing its Cybersecurity posture and FISMA rating. The Offeror's response will be evaluated holistically using the total confidence methodology.

M.3.4 Factor 5: Management Approach

The government will assess its total confidence in the Offeror's Program Management, Quality Control Approaches and Recruitment Retention and Training.

Program Management: The Government will evaluate the extent to which:

1. The approach and methodologies to the planning, execution, tracking, invoicing and reporting of the TOs awarded under this contract demonstrate sound and logical business practices.
2. The Offeror implements industry/ITIL best practices to track and report performance metrics/data regularly and builds in flexibility to provide requested metrics/data as needed in alignment with Government objectives.
3. The Offeror implements continuous improvement to gain efficiencies demonstrated through metrics/data provided.
4. The proposed project management approach and the Offeror's methodology for ensuring that cost, schedule and performance objectives, project metrics such as CPI (Cost Performance Index), SPI (Schedule Performance Index) and EVM (Earned Value Management), service-level agreements or other types of performance metrics and measures are controlled, reported, and managed.
5. The approach for managing multiple TOs demonstrates knowledge and application of project management disciplines, including:
    a. the tools and methodologies for planning the activities of its team(s),
    b. having a resource loaded Schedule, and
    c. scheduling, organizing, and deploying resources, controlling the execution of the task, monitoring progress through EVM milestones, status reporting, resolving critical issues, reporting/maintaining risk, and planning for subsequent phases of work.

6. The Offeror's governance and reporting structure provides transparency and Government access to real time performance metrics.

The Government may also evaluate the Offeror's proposed Program Manager to determine whether their experience is commensurate with the requirements of a contract of this size, scope, and complexity.

Quality Control: The Government will evaluate the extent to which the Offeror's Quality Control solution includes a comprehensive, verifiable, and self-implementing approach for monitoring its performance. In addition, the government will evaluate the extent to which the Offeror's process determines root cause analysis for issues/outages and take the requisite corrective action

Recruitment, Retention and Training: For the cognizant business unit (i.e., the legal entity proposing on this procurement), the Government will determine its confidence in the Offeror's ability to recruit, train, and retain high quality personnel. Emphasis will be placed on the education, professional certifications, and security credentials obtained by the workforce in relation to the number of personnel in the business unit, their average length of service, and the turnover rate experience of the business unit for the last three (3) year period.

M.3.5 Factor 6: Ability to Achieve Results through Teaming

The Government will evaluate its total confidence in the Offeror's proposed approach to achieving results through teaming and in doing so the government may evaluate the extent to which the Offeror's proposal:

1. Indicates a systematic approach to continuously seek to identify the best sources of solutions and services to meet the Department's objectives
2. Integrates partners and subcontractors into the performance plan
3. Indicates any management controls to avoid perverse outcomes beneficial to the company's bottom line but not to the Government

M.3.6 Price- TBD

M.3.8.1 Price Evaluation of Options

The Government will evaluate offers for award purposes by evaluating prices for the base period as well as all options. Evaluation of options will not obligate the Government to exercise the options. Offers containing any charges for failure to exercise any option will be rejected.

M.4 Evaluation

In its evaluation, the Government will consider the benefits and risks associated with the Offeror's proposal to arrive at a confidence assessment of the Offeror's likelihood of successfully performing the requirements of the solicitation. The table below shows the rating system the Government will use in its evaluation of all the technical evaluation factors.

Rating	Description

High Confidence	The Government has high confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing the work.
Some Confidence	The Government has some confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing the work.
Low Confidence	The Government has low confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing the work.

M.5 Contractor Support

Offerors are hereby notified that the Government may have contractors from Gartner and others provide assistance during this acquisition. The companies/organizations may have access to some of the information contained in the Offeror's proposals and will be subject to appropriate conflict of interests and standards of conduct. The company/organization is also required to comply with strict confidentiality restrictions and all personnel working on this acquisition have executed Non-Disclosure Agreements.

(End of Section M)