DEFENSE INTELLIGENCE AGENCY

COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

Statement of Work

July 2, 2020

www.dia.mil/Business/SITE-III

UNCLASSIFIED

GENERAL INFORMATION

This non-personal services contract delivers Solutions for the Information Technology Enterprise III (SITE III) to the Defense Intelligence Agency (DIA) and the National Geospatial-Intelligence Agency (NGA). The Government will not exercise any supervision or control over the service contractors performing the services herein. Servicing contractors are accountable solely to the Contractor, who, in turn is responsible to the Government.

1. Title of Project

Solutions for the Information Technology Enterprise III (SITE III)

2. Background

The Chief Information Office (CIO) mission is to provide the full range of support required to plan, maintain, and sustain the global CIO organization. The CIO seeks to exercise broad responsibility and authority for planning and to manage its operations and services.

This Statement of Work (SOW) describes the basic services contractors shall provide to support the DIA and NGA under the SITE III Indefinite Delivery/Indefinite Quantity (IDIQ) contract vehicle. This IDIQ contract establishes the acquisition framework for delivering the full scope of information technology services and capabilities to support intelligence needs for the DIA and the NGA.

This contract vehicle provides participating organizations with comprehensive Information Technology (IT) technical support services. This vehicle leverages a mix of large and small prime and subcontractor businesses to satisfy mission requirements.

The SITE III multiple award contract vehicle qualifies selected contractors to propose solutions for ensuing TOs. The Government will provide a Performance Work Statement (PWS) or Statement of Work (SOW), Cost Volume, and a Quality Assurance Surveillance Plan (QASP) for each task order. Associated performance objectives, deliverables, and thresholds will be specified in the PWS or SOW in each TO as appropriate.

3. Objective

The DIA CIO's primary objective with SITE III is to support warfighters, policymakers, and acquisition leaders across the Defense Intelligence Enterprise (DIE) by achieving an Information and Communications Technology advantage. SITE III provides strategic, technical, and program management guidance and support services to facilitate the operations and modernization of the agency's infrastructure, systems, and applications. The SITE III contract is not intended for staff augmentation. Rather,

the SITE III contract provides managed services directed towards improving integration, information sharing, and information safeguarding through the use of a streamlined information technology (IT) approach. The CIO expects innovation with common architecture, consolidated operations, and cloud environments in alignment with the Intelligence Community's Information Technology Enterprise (IC ITE) as directed by the Director of National Intelligence (DNI). Task Orders issued under SITE III must comply with Industry Standards, IC, and CIO Directives, to include memorandums and directives issued by the CIO Technical Leadership Council (TLC).

4. Scope

The SITE III IDIQ contract vehicle addresses the evolving needs vital to the security of the United States. SITE III facilitates worldwide coverage for integrated IT intelligence requirements and technical support services to the DIA and NGA.

Contractors shall provide the full range of integrated strategic, analytic, and technical support services DIA may need to design and implement optimal Infrastructure, Systems, and Applications initiatives and ensure progress toward meeting requirements and objectives. The selected contractors shall have subject matter expertise and provide all resources necessary to perform the specific requirements as defined in individual task orders.

Contractors shall develop, maintain, and periodically update Supply Chain Risk Management (SCRM) plans at no cost to the Government. SCRM plans are intended to reduce performance and security risks of the products sold, installed, and maintained throughout the life-cycle. SCRM plans shall include sufficient detail for the Government to determine that the Contractor reasonably understands its supply chain and the associated risks. The Contractor shall ensure that genuine Information and Communication Technology (ICT) will be available under the contract and shall manage the risk to ensure counterfeit or illegally modified products are not shipped. SCRM plans shall describe the processes and practices ensuring Contractors can deliver genuine ICT.

The services and capabilities supported by the SITE III contract vehicle will provide responsive, secure, and timely solutions to participating organizations that meet current and future IT requirements. Technical requirements are defined in Section 5 of this document. The SITE III contract supports both classified and unclassified programs on multiple networks and security domains. Individual task orders will identify the scope of work required for networks, domains, and security.

It is not possible for the Government to determine the precise types or amounts of services it will require during the full term of the contract. The Government will make every effort to provide the Contractor with ample time to respond to new requirements. However, some task orders on this contract may require fast responses to address emergent requirements. Services performed will be non-personal and shall not include inherently governmental services. The Government reserves the right to designate selected task orders (TOs) as set-asides for competition among small businesses.

5. Requirements

The SITE III IDIQ contract vehicle streamlines the delivery and management of application and infrastructure services and functions for current and emerging requirements. Industry partners shall have relevant experience in essential IT services and the functions listed within this document. Task orders may contain requirements for one to many of the IT services and functions listed based on a participating Government organization's requirements. Enterprise activities and services may be combined to maximize efficiencies, drive process improvements, eliminate service overlaps, evolve with leading-edge technology, and realize cost efficiencies at the task order level to provide strategic IT advantages to the US Government.

The Contractors shall provide the following:

5.1. Enterprise Activities and Services

5.1.1. Enterprise Architecture Definition, Documentation, and Planning

5.1.1.1. The Contractor shall develop the IT system architecture documentation, design, and plans of current and future technical and functional/business systems by depicting technical, systems, and functional architecture views. Services include the facilitation and development of plans that enable information sharing, integration, and interoperability by considering service-oriented architecture best practices by aligning architectures with overarching Federal, IC, Department of Defense (DoD) architectures, and other related architecture activities.

5.1.1.2. Contractors shall provide the architectural support through the full life-cycle of planning, execution and management of Enterprise data backup, Humanitarian Assistance and Disaster Response (HA/DR), Continuity of Operations (COOP), and include initial planning through systems decommissioning.

5.1.2. Technology Assessment and Evaluation

5.1.2.1. The Contractor shall provide or support researching, developing, testing, and evaluating (RDT&E) of new and emerging technology for potential insertion into current and future programs to satisfy mission requirements based on a business case analysis (e.g., cloud services or Big Data analysis). These tasks may include but are not limited to, analytical capabilities, infrastructure innovation, data innovation, and other strategic innovations. The RDT&E shall comprise of practices that enable rapid fielding of capabilities developed externally, including the establishment of a Continuous Integration/Continuous Delivery (CI/CD) methodology and a systematic, repeatable, secure, and streamlined delivery of capabilities to production environments.

5.1.3. Independent Testing and Verification

5.1.3.1. The Contractor shall provide management and operational support for enterprise independent testing activities designed for system, application, and service-oriented IT functions to uncover operational software, hardware, and/or system flaws before fielding to reduce and eliminate erroneous products or mission failure. Activities

associated with these efforts include, but are not limited to, establishing evaluation criteria and conducting evaluations for applications; ensuring security controls are aligned with the assessment & authorization and audit processes, and applications comply with risk management authorization process in accordance with IC Directive 503, DoD Instruction 8500 (i.e., IA Controls, Cyber Security), IC Standard 500-27 audit data, and Other relevant DoD and IC Cyber Security/Security policies, implementing a centrally managed test process, documenting testing requirements for evolving service-oriented architectures, participating in mission application in-plant acceptance testing and beta tests, working with functional users that the test processes address user requirements and issues, and establishing a library of widgets that link to documented test processes plans and procedures for enhancement and reuse on various mission applications.

5.1.4. Project Management and Planning

5.1.4.1 The Contractor shall provide project management and planning services with the capability to manage large projects applying the Project Management Institute (PMI) best practices (e.g., Project Management Body of Knowledge, (PMBOK), Guide & Standards, and IC agency-level software development lifestyle standards.

5.1.4.2 The Contractor shall provide Information Technology Infrastructure Library (ITIL) Service Management Framework (Version n and any subsequent revisions), and guide provisioning of the services and the processes, functions, and other capabilities needed to support them. Apply current industrial software development best practices that contain iterative and incremental project management techniques similar to the agile software development life cycle standards while utilizing DIA's Risk Management Framework (RMF). The Contractor shall provide for processes and functions across the entire ITIL life-cycle (Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement); organizations may call out specific ITIL process and functional requirements within follow-on task orders to support their IT operating models.

5.1.5. Logistical Support and Inventory Management

5.1.5.1. The Contractor shall perform associated logistical support and inventory management functions to maintain and track equipment and software accountable (unless provided as Government furnished equipment) under the contract. This task includes acquiring and managing all parts and materiels necessary to support the actions required as specified in task orders. Logistics support and inventory management includes but is not limited to, the equipment, spares, and licensing inventory management, shipping and receiving, ordering, tracking, shipping, expediting purchases, warehousing, storage, and staging.

5.1.5.2. The Contractor shall develop and implement techniques, processes, and procedures to maintain a "just-in-time" inventory methodology, which ensures customer fulfillment while reducing warehousing cost of storage. The vendor shall analyze and recommend updates, enhancements, or replacements to extend the life or improve the reliability of critical equipment or equipment no longer supportable by repair or replacement. Contractors shall have written Government approval prior to the implementation of

recommendations and purchases in accordance with all Federal, DoD, and DIA contracting regulations. Recommended updates shall support integration with existing systems and dashboards at DIA, ensuring a centralized view of logistical support, inventory management, and records maintenance in accordance with DIA, Office of the Director of National Intelligence (ODNI), and DoD policies to support audit requirements.

5.1.6. Asset and Configuration Management

5.1.6.1. The Contractor shall provide current architectures comprised of separate disparate client server legacy, virtual, and cloud environments. The Government will migrate and transition to a hybrid architecture with a heavy emphasis on virtual and cloud environments. Asset and configuration management are defined differently for each of environment. The work includes asset management and configuration management (CM) services to maintain technical and administrative control of the functional and physical characteristics of technology assets. It also provides continuous visibility into the types and numbers of assets throughout the enterprise. The work includes identification and definition of the IT configuration items (CIs) in the system and control the change of these items throughout their life-cycle as well as report status of a CI during its life cycle. The work objectives include supporting and conducting periodic change boards or other CM-related meetings. The work includes managing the status accounting process, facilitating status review and change boards, document review board results, and follow up on action items from the CM-related meetings. The Contractor shall integrate with existing systems and Dashboards to ensure DIA maintains a continuous centralized view of asset and configuration management and eliminates hierarchical and organizational information flow constraints, also known as stovepiping.

5.1.7. Knowledge Management, Technical Writing and Document Support

5.1.7.1 The Contractor shall provide technical writing and documentation support. Technical Writing Services and Documentation Support include but are not limited to, supporting technical staff in the development and dissemination of technical documents including requirements analyses, design documents, manuals, fielding documents, and network security documents. This task includes preparing contract deliverables and reports, assisting in the preparation of presentation graphics and supporting the development of deliverables and reports, and maintaining configuration management control of all documents.

5.1.8. Enterprise Operations, Event Monitoring and Management, Performance Monitoring, and Analysis

5.1.8.1. The Contractor shall conduct enterprise operations, event monitoring and management, performance monitoring, and analysis services. The Contractor shall provide continuous centralized operations, monitoring, management and analysis of enterprise applications, systems, and core services as well as infrastructure assets to include file servers, email servers, application servers, web servers, and storage for all enterprise service providers 24 hours per day, seven days per week to include holidays. Contractor services shall include but are not limited to, monitoring established thresholds,

responding to warning and alert messages from the monitoring systems, coordinating corrective action once thresholds are reached to prevent issues from reoccurring, and conducting the initial troubleshooting to restore services as quickly as possible. Other services include providing feeds to the enterprise watch and other Governmentdesignated watch centers as directed for situational awareness, responding to escalated incidents and outages (e.g., from the service desk), taking corrective actions to resolve the issue, escalate unresolved issues, maintaining, and upgrading the supporting network infrastructure and services.

5.1.9. Information Technology Service Management

5.1.9.1. The Contractor shall conduct Information Technology Infrastructure Library (ITIL) Service Management Framework (Version *n* and any subsequent revisions) guide provisioning of the services and the processes, functions, and other capabilities needed to support them. The Contractor shall provide processes and functions across the entire ITIL life-cycle (Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement). Supported Government organizations may call out specific ITIL processes and functional requirements within follow-on task orders to support their IT operating models.

5.2. Infrastructure Development/Sustainment

5.2.1. Customer and Work Center Support Services

5.2.1.1. The Government requires Contractor assistance at all phases of the IDLC with refining requirements, securing design, and integrating hardware and software. The Contractor shall have the capability to test, distribute, use, maintain, and dispose of hardware and software. The Contractor provided services shall include but are not limited to, local and worldwide engineering and installation management, conducting site surveys, estimating bills of materiels, estimating timelines, recommending hardware and cabling technical solutions, ensuring security controls and authorizations are in place, documenting project status and the installation "as-is" and "to-be" architectures, planning, building, and installing patch panels and cable/fiber infrastructures, installing and terminating all types of standard IT cable and fiber, data center racks, fiber framework, server, storage, and networking equipment, deploying IT capabilities (e.g., workstations, desktops, printers, and peripherals, Voice Over Internet Protocol phones, video displays, and video teleconferencing) to customer workspaces, and decommissioning and removal of legacy equipment or infrastructure that are no longer required. The specific IT Infrastructure Installations, Fit Outs, and decommissioning requirements and services will be identified within individual task orders.

5.2.1.2. The Contractor shall develop Service Desk capabilities include customer self-help services, online support services, and customer representative services. The configuration of the Service Desk, supported by a one-number-to-call, can be either an integrated federated system of existing Agency service desks or a traditional consolidated physical Service Desk. The Service Desk shall be the central point of contact for the customer and the IT organization for resolving customer IT issues at the lowest practical support level. Service Desks shall provide a consistent and quality customer experience across enterprise service areas using qualified staff, standardized

processes, and an extensive knowledge management system. The Service Desk, supported by a common Information Technology Service Management (ITSM) toolset, shall provide the ability to document, process, and monitor incidents, problems, inquiries, and change and service requests, as well as coordinate new capabilities through an actionable service catalog and support for other IT service management functions. The Service Desk shall provide customer support and other required services 24 hours per day, seven days per week, including holidays. Specific Service Desk requirements and services will be identified within individual task orders.

5.2.1.3. The Contractor shall provide customer desk-side support services for end-users and customer work center environments. Services include but are not limited to, providing desk-side assistance to resolve customer incidents, locally resolving system account and access management issues. The Contractor shall tailor directory service entries, organizational mailboxes, distribution lists, etc., to meet customer requirements. The Contractor shall install Government approved add-on applications to workstations, and support equipment installation, move, add, and change requests. The Contractor shall configure, troubleshoot, and maintain end-user devices and peripherals. In support of the enterprise, Contractor services may include initial troubleshooting analysis and resolution for server and storage, installing patches and performing system updates, recovering data, and installing and configuring server and storage devices.

5.2.1.4. The Contractor shall provide Field Service Support at designated Government locations within the Contiguous United States (CONUS) or outside the contiguous United States (OCONUS). Services include providing general IT support across a wide range of technical services. Field service technical support includes but is not limited to, operating an entire site remotely, providing IT support services at remote field and garrison sites, performing basic cabling and server/desktop installation, performing systems administration of desktop and server systems connected to local and wide area networks, supporting VTC operations, maintaining and loading cryptographic keys, and performing troubleshooting on many types of hardware and software.

5.2.2. Connectivity and Network Services

5.2.2.1. The Contractor shall provide Connectivity and Network Service Delivery Life-cycle support for the DIA global enterprise architecture at designated Government locations. Connectivity and Network services require a wide range of technical, functional, and program management services to support full engineering, design, cybersecurity, integration, installation operations, and maintenance activities of all classified and unclassified, wired, wireless, and tactical satellite communications network services and capabilities.

5.2.2.2. The Contractor shall provide Connectivity and Network service requirements to include but not limited to, architecture and engineering development and design, cable and fiber installation, testing, troubleshooting and management, full wide-area, metropolitan area, campus area, local area, and data center network administration, network operations, event monitoring and management, performance monitoring, capacity planning, and analysis, Internet Protocol Address Management (IPAM) and Network Timing Protocol (NTP) systems and tools administration and maintenance, ITSM systems and tools administration and maintenance, incident response, tracking, and

resolution, Communications Security (COMSEC) account, key material, installation, management and support services. Compliance with current DoD and IC policies, standards, and security directives and guidelines.

5.2.2.3. The Contractor shall provide certified cybersecurity expertise (i.e., Information System Security Engineers (ISSE) or Information Systems Security Officers (ISSO), as appropriate) throughout the design, engineering, and installation processes to ensure proper security controls are in place and validated. The Contractor shall ensure IT architecture and networks are interoperable with computer network defense (CND) capabilities. The Government will identify specific Connectivity and Network requirements and services in the individual task orders.

5.2.3. Enterprise Computing, Storage, & Cloud Services

5.2.3.1. The Contractor shall provide Enterprise Computing, Storage, and Cloud Service Delivery Life-cycle support for the DIA global enterprise architecture at designated Government locations. Enterprise Computing, Storage, and Cloud services require a wide range of technical, functional, and program management services to support full engineering, the design, integration, installation operations, and maintenance activities of all classified and unclassified, compute, storage, cloud, physical and virtual infrastructure components.

5.2.3.2. The Contractor shall provide Enterprise Computing and Storage services to include but not limited to, creating, accrediting and maintaining server and workstation baselines for all supported operating systems on all networks, standardizing , deploying, and patching for all systems in operations, repairing and maintaining hardware and software, administering and managing server and storage, providing data services, data administration, and database management, providing infrastructure system services, administration, and management support for traditional systems and systems that use virtual and cloud services hosted by other agencies or external cloud service providers that provide Platform as a Service (PaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS) capabilities; operating, maintaining, and sustaining enterprise shared applications and infrastructure services (e.g., email, SharePoint, Identity Management, Directory Services, Public Key Infrastructure (PKI), Global Load balancing Traffic Management), providing event monitoring and management, performance monitoring, capacity planning, and analysis; and providing incident response, tracking, and resolution.

5.2.3.3. The Contractor shall provide certified cybersecurity expertise (i.e., Information System Security Engineers (ISSE) or Information Systems Security Officers (ISSO), as appropriate) throughout the design, engineering, and installation processes to ensure proper security controls are in place and validated. The Contractor shall ensure IT architecture and networks are interoperable with computer network defense (CND) capabilities. The Government will identify specific Enterprise Computing, Storage, and Cloud requirements and services in the individual task orders.

5.2.4. Mission and Business Systems Services, Administration, and Management

5.2.4.1. The Contractor shall provide administration and management of mission and business system services for both traditional systems and systems that exist within or use virtual and cloud services hosted by other agencies and external cloud service providers. These services include but are not limited to, applications, databases, system-level administration functions for enterprise, regional, and Combatant Command intelligence mission applications and business systems. The services also include providing certified cybersecurity expertise (ie. ISSE or ISSO as appropriate) throughout design, engineering, and deployment to ensure proper security controls are in place and validated, and to ensure the systems and services are interoperable with CND capabilities. Specific mission and business systems services, administration, and management requirements will be documented in individual task orders.

5.2.5. Unified Communications, Voice, Video, and Chat Services

5.2.5.1. The Contractor shall provide Unified Communications, voice, video, and chat service delivery life-cycle support for the DIA enterprise. Unified Communications Voice, Video and Chat services require a wide range of technical, functional, and program management services to support full engineering, design, integration, installation operations, and maintenance activities of all classified and unclassified capabilities.

5.2.5.2. The Contractor shall provide Unified Communications, voice, video and chat services that include but are not limited to, integrating real-time communications services with non-real time communication service, non-secure and secure voice installation, providing operations and maintenance services, configuring and managing automated call distribution systems, call managers, and other tools required for administration, providing incident response, tracking, and resolution, performing service operation activities such as troubleshooting, event monitoring and management, performance monitoring, capacity planning, and analysis, designing, installing and maintaining all ADHOC and scheduling conferencing capabilities, installing, operating and maintaining all desktop video, studio video, and video teleconferencing (DVTC and SVTC) services, and provide user Mobility Capability.

5.2.5.3. The Contractor shall provide certified cybersecurity expertise (i.e., ISSE or ISSO as appropriate) throughout the design, engineering, and deployment to ensure proper security controls are in place and validated, and to ensure the systems and services are interoperable with CND capabilities. The Government will identify the Unified Communications, voice, and video requirements and services in individual task orders.

5.2.6. Audio Visual and Digital Media Services

5.2.6.1. The Contractor shall provide audio, visual and digital media service delivery life-cycle support for the DIA Enterprise. Audio, visual, and digital media services require a wide range of technical, functional, and program management services to support full engineering, design, integration, installation operations, and maintenance activities of all classified and unclassified capabilities.

5.2.6.2. The Contractor shall provide audio, visual, and digital media services that include but are not limited to, engineering, installing, and programming video display and knowledge wall systems, conducting routine operational tests and fault isolation on video display

systems, optimizing system operation and resource utilization, providing assistance to users in using systems, maintaining and operating a wide variety of video display equipment to include video streaming devices, channel and layout controls, audio and video display components, related tools administration and maintenance, service operation activities, troubleshooting, event monitoring and management, performance monitoring, analysis and capacity planning, and continuously monitoring all component equipment.

5.2.6.3. The Contractor shall provide certified cybersecurity expertise (i.e., ISSE or ISSO as appropriate) throughout the design, engineering, and deployment to ensure proper security controls are in place and validated, and to ensure the systems and services are interoperable with CND capabilities. The Government will identify specific Audio Visual and Digital Media requirements and services in individual task orders. See Section 5.6 for Cybersecurity Services requirements.

5.3. Application Development and Sustainment

5.3.1. Customer and Work Center Support Services

5.3.1.1. The Contractor shall provide comprehensive customer relationship management (CRM) services. CRM supports the overall need for a balanced blend of quality and cost efficiency regardless of the end state. The Contractor shall provide customer outreach and relationship management services that effectively facilitate communications between participating IT organizations and their customers. The Contractor shall support, develop, and implement improvements to the CRM framework that ensure customers are adequately supported throughout the service life-cycle within the context of the hybrid environments.

5.3.1.2. The Contractor shall conduct mission engagement and operations planning to provide a critical linkage between customer mission planning and IT support planning. Services include but are not limited to, operations planning (OPLAN), contingency planning (CONPLAN), exercise support planning, defining and documenting customer "as is" and "to be" architectures, creating and monitoring customer service-level agreements, and analyzing operational performance measurements and associated trends to ensure services meet customer missions, goals, and objectives.

5.3.1.3. The Contractor shall provide or support Customer Education and Training services to include providing for the principles, and techniques of instructional design methodology to develop and deliver training materials and programs as well as provide customized education and training to CIO customers in varied venues and locations. Training requirements may include, but are not limited to, “train the trainer,” classroom, or virtual courses. Training materials may include but are not limited to, user guides, training manuals, instructor manuals, and reference guides. Customer feedback shall be collected at the end of training and reported following the completion of training.

5.3.2. Mission and Business Application, Tools, Portals, and Web Services

5.3.2.1. The Contractor shall provide or support Software Engineering, Development, and Integration using the Agile development methodology (rapid development with embedded security) testing environment to assess the direction of a project during the life-cycle development through abbreviated regular cadences of work known as sprints or iterations. The Contractor shall focus on the repetition of abbreviated work cycles as well as task order functional requirements, quality, and security expectations.

5.3.2.2. The Contractor shall provide support for the legacy and virtual IT environments. The Contractor shall provide Software as a Service (SaaS) expertise to develop applications to run on a cloud infrastructure in accordance with Government defined standards and within Government defined frameworks. The applications shall be accessible from various client devices through a thin client interface such as a web browser (e.g., webbased email). The Contractor shall perform requirement capture and analysis, requirements specification creation, software design, development, integration and testing, version control, project management, and problem tracking and solutions. The Contractor shall provide for configuration, installation, deployment, account migration services, follow-on operations, and maintenance on an end-to-end basis throughout all networks.

5.3.2.3. The Contractor shall provide certified cybersecurity expertise (i.e. Information Systems Security Officers or Engineers (ISSO/ISSE)) throughout the design, engineering, development and deployment to ensure proper security controls are in place and validated.

5.3.2.4. The Contractor shall provide Mission and Business Application and Tool Development, Integration, and Maintenance services focused on designing, developing, integrating, and maintaining applications, tools, services, and other software to improve business and mission capabilities and improve application effectiveness. Contractor services shall include but are not limited to, developing new enterprise applications, implementing enterprise applications services to raise intelligence product quality and expand information sharing, adding, modifying, deleting functionality based on customer requirements, and integrating new application architectures, upgrading and depreciating software and support tools as newer versions are released, improving application and tool quality and performance, and migrating legacy applications and tools to enterprise applications and tools.

5.3.2.5. The Contractor shall use Government provided software and tools to perform Mission and Business Application, Tools, Portals, and Web services to the maximum extent possible. Where cost efficiencies and innovation may be achieved, Contractors shall incorporate other software and tools in accordance with ITSM methodology and principles, including the reuse or integration of Government-owned software, such as those from Research and Development (R&D) technology insertions and from mission partners.

5.3.2.6. The Contractor shall provide certified cybersecurity expertise (i.e., ISSO/ISSE) throughout design, development, and deployment to ensure proper security controls are in place and validated.

5.3.2.7. The Contractor shall provide web and portal systems development, integration, maintenance, and management services. Support services shall include but are not limited to, web and web portal planning, development, integration, testing, and support as defined in individual task orders. Work performed shall ensure web systems and portals integrate effectively with existing enterprise systems and data stores with the goal of maintaining a well-connected, secured, and controlled enterprise of systems. Services shall follow the structured development, test, and release management processes in addition to stringent change management and configuration control and enforcement of service level agreements. In addition to supporting current and future mission requirements for web and portal services and data sharing task orders will require the implementation of web services standards such as the Intelligence Community Metadata Standards for Publications as well as providing key security and management capabilities necessary to ensure quality of service, uptime, and monitoring of security threats to bring about better control over and visibility of web and portal services.

5.3.2.8. The Contractor shall perform application and portal support for data analytics, development, integration, and management. Services for data analytics to include, but are not limited to, the development, integration with existing DIA systems, maintenance, of descriptive, diagnostic, predictive and prescriptive analytics. Applications and services shall include the interpretation of historical data, using statistics and modeling to determine future performance, use of artificial intelligence and other emerging technologies to help DIA make better decisions by factoring in knowledge of possible situations. The Contractor shall develop and promote data analytics technology innovation that results in greater mission impact. Performance in this area shall support development, deployment and operations of a variety of multiINT, advanced data analytics and data science missions, using DODIIS and IC ITE at the Unclassified, Secret and Top Secret development environments, address systemic intelligence problems to collect, analyze, exploit and store mission data to achieve mission objectives through the application of data science innovations such as Machine Learning, Artificial Intelligence (AI) and Data Analytics technology.

5.3.2.9. The Contractor shall provide content management to support a collaborative culture and enterprise as part of its web presence. Services focus on end-user support to include tailoring front-end interfaces for intelligence mission and business applications as well as web portal presentation and content customization (i.e., portlets, digital authoring, and web publishing, tasking systems). Services should enable customer use of supported intelligence mission and business applications and their business processes in all IT environments. Content management services shall ensure systems integrate effectively with existing enterprise systems and data stores with the goal of maintaining a well-connected, secured, and controlled enterprise of systems.

5.3.2.10. The Contractor shall provide Knowledge Management support services to support the institutional knowledge of people, processes, and systems to the right customer at the right time by integrating existing systems and dashboards that ensure DIA has a centralized and managed view.

5.3.2.11. The Contractor shall provide or support the development and test environment. The development and test environment provides the capabilities necessary to functionally

verify, perform regression testing, and confirm the interoperability of mission and business applications, tools, and web and portal services prior to promoting into the operational baseline. The preceding applies to all networks. Work in this area supports standard development and test environments, tools, and processes to facilitate maintenance releases, interoperability, and speed of application delivery for the full life cycle of delivered applications.

5.3.2.12. The Contractor shall provide or support Life-Cycle Software License Management and Control. Life-Cycle Software License Management and Control capabilities define, track, and control licenses procured under the contract and those licenses provided by the Government for the full period of performance of the contract. This capability should be online/remotely accessible through standard features (e.g., browser) to provide the Government situational awareness and ensure compliance with applicable license terms and conditions. The Contractor shall integrate with existing software lifecycle license management systems and dashboards at DIA to support a centralized view and eliminates hierarchical and organizational information flow constraints, also known as stovepiping.

5.4. Other Special Services

5.4.1. Outside Technical Support Services

5.4.1.1. Due to the specific missions of various sites, the need for specialized outside technical services sometimes accompanies or supplements the primary requirements supported by the individual task orders. When necessary, the Contractor shall obtain specialized computer-related technical services. These services are of a nature that could not reasonably be expected to be provided by the Contractor on a full or part-time basis. Examples of such services are those from hardware or software manufacturers or other subject matter experts in unique or specialized areas or technologies (e.g., access to Microsoft, Sun, Dell, etc. for higher levels of support may be required).

5.4.2. Call-Out or Per-Call Support Services

5.4.2.1. The Contractor shall provide the capability of Call-Out or Per-Call support for very short duration requirements. Situations when Call-Out/Per-Call support may include but are not limited to, no personnel are available in an affected area (e.g., network node outage) to provide restoration services, on-site personnel are not available to provide the required service, or on-site personnel do not have the specialized service or technical expertise. Call-Out/Per-Call support requirements shall be provided in individual task orders.

5.4.3. Surge Support Services

5.4.3.1. The Contractor shall provide surge support for limited duration requirements that cannot be accomplished by on-site personnel. Examples of surge support include, but are not limited to, installation or de-installation of equipment, disaster recovery efforts, contingency operations support, exercise support, or site relocation support. The Government will provide the Contractor notification of surge support requirements,

including locations, durations, specific services required, suggested number of personnel, and any other surge unique information. The Contractor shall determine and provide any additional task order costs to the Government. The Contracting Officer must approve any additional costs prior to the Contractor executing a surge support requirement.

5.4.4. Deployment Support Services

5.4.4.1. The Contractor shall provide deployment support services ranging from supporting and repairing equipment deployed to a location other than the location to which it is primarily assigned to or deploying Contractor personnel to a theater of operations to support training missions, exercises, contingencies, or crisis situations. The Government will define Contractor functions that may be deployable within specific task orders. Contractor personnel performing these functions shall accomplish all required deployment processing and receive all necessary deployment training and protective equipment in accordance with the participating organization's processes outlined in the task order. The Contractor shall provide employees who are medically fit and capable of enduring the rigors of deployment in the designated theater of operations. The Contractor shall comply with all deployment requirements established by the Theater Commander, including immunization and medical screening.

5.5. Support Core Functions

5.5.1. The Contractor shall improve performance in the following core functional areas:
5.5.1.1. Intelligence Support to Acquisition
5.5.1.2. Intelligence Mission Data
5.5.1.3. Warning
5.5.1.4. Targeting
5.5.1.5. Collection Management
5.5.1.6. Foundational Military Intelligence (FMI),
5.5.1.7. Scientific and Technical Intelligence (S&TI)

5.6. Cybersecurity Services

5.6.1. The Contractor shall provide Cybersecurity services that enforce, comply with, and support the DoD and IC Cybersecurity directives, policies, and procedures. Cybersecurity services include a wide range of technical, functional, operational, and managerial services necessary to ensure the secure operation of systems and networks.

5.6.2. The Contractor shall provide Cybersecurity services to include but are not limited to, policy development, Security technical assessment, insider threat assessment, security architecture development, security engineering, authorization recommendations, and security compliance (such as ICD 503 and ICD 705, DoDI 8500 controls, IC Standard 500-27, and other relevant DoD and IC policies).

5.6.3. The Contractor shall provide Cyber Security training management in accordance with DoDD 8140.01, user attributable enterprise auditing, assessment, and reporting services, cybersecurity Service Provider (CSSP) in accordance with DoDD 8530.1, Chairman of the Joint Chief of Staff Instructions (CJCSI) 6510.01E, and CJCSM

6510.01, and ICD 502 vulnerability assessment and management, metrics consolidation and reporting on DoD and IC mandatory reporting (to include the Federal Information Security Management Act (FISMA), Federal Information Systems Controls Audit Manual (FISCAM), and Inspector General requirements), cybersecurity and IT systems and tools administration and maintenance, cross-domain solutions support, inter-agency coordination, and PKI procedures and guidance.

5.6.4. The Contractor shall provide Cybersecurity requirements and services supporting infrastructure programs as identified in the individual task orders.

6. Deliverables

6.1. The Contractor shall provide written progress reports as outlined in the Contract Deliverable Requirements List (CDRL) for the period each task order. Reports shall cover all work completed during the specified task order period of performance and shall represent the work to be accomplished during the subsequent period. These reports shall identify any problems and a statement explaining how the problem was or is to be resolved. These reports shall be submitted via the Joint Worldwide Intelligence Communications System (JWICS).

6.2. All information and data related to this contract gathered or otherwise obtained by the Contractor shall be protected from unauthorized release and considered the property of the Government. The Contracting Officer may authorize release any data, the draft deliverables, the final deliverables, or any other written or printed materials pertaining to this contract verbally or in writing. Press releases, marketing material, or any other printed or electronic documentation related to this contract, including the association of the vendor with this contract, shall not be publicly released without the written approval of the Contracting Officer.

7. Government Furnished Property, Materiel, Equipment, or Information

7.1. The Government will provide Contractor employees with the following property at their assigned work locations:

7.1.1. Access to Non-classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), and the Joint Worldwide Intelligence Communications System (JWICS) networks and systems access, including printers and digital senders.

7.1.2. Contractor employee use of DoD computers is FOR OFFICIAL USE ONLY. Government computer use is subject to monitoring at all times. All data generated or collected on DIA computers are the property of the U.S. Government and the release, downloading or transmittal of data is subject to Government approval. Contractor personnel are not authorized to introduce computer hardware, software, or data storage media (physical or digital) into a Government facility, computer, or network device without the prior written approval and notification of the appropriate Government authorities. All downloading and transmission of information within DIA's custody is prohibited except as provided for in the terms of this contract.

7.1.3. Additional GFP, material, equipment, and information may be provided at the Task Order level.

8. Travel

8.1. Contiguous United States/Outside the Contiguous United States (CONUS/OCONUS) travel may be required in the performance of this contract. All travel shall be approved in writing by the Contracting Officer Representative (COR) prior to making any reservations. Contractors shall consult the Defense Travel Management Office website (www.defensetravel.dod.mil) prior to traveling to obtain updated per diem rates for the locality to which they are traveling.

8.2. Travel and Per Diem Rates

8.2.1. Travel costs will be allowed to the extent that they are reasonable and allocable. All travel will be reimbursed in accordance with the Federal Travel Regulation (FTR) and the Joint Travel Regulations (JTR).

8.2.2. The per diem allowance will not be allowed when the period of official travel is ten (10) hours or less during the same calendar day. Travel by privately owned vehicle shall be reimbursed at the current GSA approved mileage rate. Current travel policy and per diem rates may be obtained at the following Internet site: http://www.defensetravel.dod.mil/site/perdiem.cfm

8.3. Travel Reimbursement

8.3.1. Only those travel costs incurred by the Contractor for contracted personnel assigned and working under this SOW will be reimbursed for the following expenses:

8.3.1.1. Contractor employee airline tickets, per diem, and miscellaneous incidental expenses incurred while on official travel will be reimbursed at actual costs in accordance with the JTR.
8.3.1.2. Per Diem is not authorized within the designated Address of Record (AOR) unless prior written approval is granted by the COR;
8.3.1.3. Per Diem is authorized during pre-deployment training;
8.3.1.4. Per diem and travel costs will be reimbursed;
8.3.1.5. Incidentals and miscellaneous expenses will not be reimbursed;
8.3.1.6. Regardless of amount, all travel costs shall be documented via copies of the original travel receipts, to be provided with the invoice requesting payment, providing the following information: traveler's name, date and place (city, town, or other similar designation) of the expenses, purpose of the trip, and expense incurred.

8.4. Local Travel

8.4.1. Local travel within 50 miles of duty location will not be reimbursed.

9. Place of Performance

9.1. The place of performance shall vary between the Contractor's facility and the government facility. The place of performance will be defined by individual task orders. Accordingly, reimbursable travel and per diem for the Contractor's employees performing work on a regular basis at the designated place of performance is not authorized.

10. Duty Hours

10.1. Duty Hours (CONUS): The core work hours of operations for all personnel assigned within the National Capital Region (NCR) are Monday through Friday (0900 – 1430) hours. A 40-hour workweek is anticipated for the Contractor personnel. However, the week may be extended to meet operational needs with prior, written, COR approval. The Program Manager shall obtain COR written approval prior to any performance in excess of 40 hours per week to ensure funding availability.

10.2. Contractor personnel assigned to Combatant Commands (CCMDs) and other national agencies outside of the NCR shall adhere to the supported headquarters core hours at their assigned location.

10.3. Duty Hours (OCONUS): Contractor employees supporting OCONUS contingency operations shall work twelve (12) hours per day, seven (7) days per week, and eightyfour (84) hours per week from Monday through Sunday. In non-contingency locations, Contractor employees shall work eight (8) hours per day, five (5) days per week, and forty (40) hours per week from Monday through Friday. Contractor personnel shall not exceed the designated work weeks without the COR's prior written approval.

10.4. Any variations to the hours will be determined at the task order level.

11. Contractor Personnel Requirements – Core Personnel

11.1. Core Personnel shall be designated in writing and shall provide written notice to the Contracting Officer at least thirty (30) calendar days prior to substituting/removing individuals occupying the following key personnel positions:

11.1.1. The SITE III Program Manager is the lead point of contact for the IDIQ Contract. The Program Manager is responsible for coordinating all operations and maintenance services. The Program Manager works in close collaboration with the COR for contract changes.

11.1.2. The Deputy Program Manager will assist the Program Manager to ensure all Task Orders move together toward meeting established goals and objectives.

12. Security Requirements

12.1. See DD Form 254 form Contract Security Classification Specification and Security Continuation Pages.

13. Information Security

13.1. All persons performing work under this contract shall protect and safeguard information in accordance with DoD and DIA directives, instructions, and procedures. These same persons shall immediately report any deviation or violation of this guidance, or any unusual or suspicious activity to the DIA Security Office. These same persons shall provide assistance and full cooperation in any subsequent investigations or inquiries conducted by DIA or other governmental agencies.

14. Training

14.1. Contractors shall complete all DIA-mandated initial, annual, refresher, and ad hoc training, to include mandatory role-based training.

14.2. Cybersecurity professionals are required to be trained and certified in compliance with current DoD Cyberspace workforce management and certification guidance, including DFARS Section 252.239-7001, DFARS Subpart 239.7102-3, DoD Directive 8140.01, DoD Manual 8570.01, and future replacement documents.

14.3. All contract personnel shall complete government-directed training, education, or experience requirements for any function identified as requiring specialized training, education, or experience. Mandatory requirements include but are not limited to functions that are identified by the government as Cyber Security, Information Assurance, and Cyberspace Workforce functions. The Contractor shall maintain currency with all mandated and successor training, education, and experience requirements during the course of contracted services, to include adherence to DoD 8570.01-M and its successor guidance. Contract personnel who do not meet the minimum government-defined training, education, and experience requirements shall not be engaged on contract. If government-mandated training, education, and experience requirements change during the course of the contract, the Contractor shall ensure all contract personnel meet the updated requirements at the Contractor's expense. Contract personnel who do not have proper and current certifications will be denied access to DoD information systems for the purpose of performing cybersecurity, information assurance, and cyberspace functions.

14.4. Contractors awarded a contract subject to this solicitation shall participate in an introduction meeting within 30 calendar days of the issuance of the IDIQ. Participation in the introduction meeting will satisfy the Government’s minimum guarantee requirement identified in Section B, “Supplies and Services and Price/Costs.”

15. Non-Disclosure Requirements

15.1. All Contractor personnel (prime and subcontractor) shall sign a Non-Disclosure Agreement in accordance with DFARS 227.7103-7 prior to beginning performance. The Contractor is bound by all NDAs signed by its employees. In the event a Contractor employee violates any of the terms of the NDA, the Contractor will be considered in breach of contract. A breach may result in a termination for default.

16. Acronym List

AOR	Address Of Record
AV	Audio Visual
BOMs	Bills Of Materials
CAP	Contractor Acquired Property
CCMD	Combatant Commands
CDRL	Contract Deliverable Requirements List
CIO	Chief Information Office / Officer
CIs	Configuration Items
CJCSI	Chairman of the Joint Chief of Staff Instructions
CM	Configuration Management
CND	Computer Network Defense
COMSEC	Communications Security
CONUS	Contiguous United States
COOP	Continuity Of Operations
COR	Contracting Officer Representative
CSSP	Cybersecurity Service Provider
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DR	Disaster Recovery
DVTC & SVTC	Desktop Video, Studio Video, and Video Teleconferencing
FAR	Federal Acquisition Regulation
FBO	FedBizOpps
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Management Act
FTR	Federal Travel Regulation

GFE	Government Furnished Equipment
GFP	Government Furnished Property
IaaS	Infrastructure as a Service
IAW	In Accordance With
IC	Intelligence Community
IC ITE	Intelligence Community's Information Technology Enterprise
ICD	Intelligence Community Directive
IDIQ	Indefinite Delivery/Indefinite Quantity
IS	Information Security

IT	Information Technology
JIT	Just-In-Time
ITSM	IT Service Management
JTR	Joint Travel Regulations
JWICS	Joint Worldwide Intelligence Communications System
KO	Contracting Officer
MAIDIQ	Multiple Award IDIQ
MSR	Monthly Status Reporting
NCR	National Capitol Region
NDA	Non-Disclosure
NIPRNet	Non Secure Internet Protocol Network
OCONUS	Outside the contiguous United States
ODNI	Office of the Director of National Intelligence
P/T	Part-Time
PaaS	Platform as a Service
PCB	Periodic Change Boards
PKI	Public Key Infrastructure
PM	Program Management
PMBOK	Project Management Body of Knowledge
POC	Point Of Contact
POTS	Plain Old Telephone Service
PPR	Price Proposal Reporting
PROSERV	Professional Services
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QBR	Quarter Business Review
RDT&E	Research, Development, Test and Evaluation
RFI	Request for Information
SaaS	Software as a Service
SB	Small Businesses
SCIF	Sensitive Compartmented Information Facility
SDS	Service Delivery Standard
SIPRNet	Secure Internet Protocol Network
SITE III	Solutions for the Information Technology Enterprise III
SME	Subject Matter Expertise / Expert
SOW	Statement Of Work
SRCB	Status Review and Change Boards

STE	Secure Telephone Equipment
TOs	Task Orders
TS/SCI	Top-Secret Sensitive Compartmented Information
VoIP	Voice-over Internet Protocol