General Requirements

For

Advancing Artificial Intelligence Multiple Award Contract (AAMAC)

CDAO

Department of Defense
Chief Digital and Artificial Intelligence Office
27 January 2025

Table of Contents

1.0 Introduction

The Department of Defense's (DoD) Chief Digital and Artificial Intelligence Office (CDAO) is the lead organization responsible for accelerating DoD's adoption of data, analytics, and artificial intelligence (AI) to generate decision advantage, from the boardroom to the battlefield.

Stood up in February 2022 by integrating the Joint Artificial Intelligence Center, Defense Digital Services, the Chief Data Officer, and the enterprise platform Advana into one organization, the CDAO's mission requires it to continually build and field strong data management, analytic, and AI-enabled capabilities for the DoD.

CDAO itself implements numerous Deputy Secretary of Defense-directed initiatives (i.e., Pulse and Campaign Decision Support analytics tools) while also sponsoring enterprise data management capabilities and applications across several functional areas (e.g., logistics, personnel, incident response) through a variety of data, analytics, and AI platforms.

As the DoD looks to scale adoption of its enterprise data management, analytics, and AI capabilities, the CDAO is designing a vehicle that will enable it to continually build high priority, high impact products, while also providing DoD organizations a flexible pathway to acquire digital capabilities for their business needs. As such, to support the vast size of DoD and the accelerated pace of change in the hi-tech industry, the requirements herein are defined broadly and intended to build a highly diverse vendor ecosystem that will enable the DoD to generate decision advantage at scale, today and tomorrow.

2.0 Scope

2.1 Overview

The broad technical scope defined herein establishes the scope of work that may be implemented through specific delivery orders (DO) or task orders (TO) or issued from this indefinite-delivery, indefinite-quantity multiple award contract (IDIQ MAC).

This IDIQ will support potential projects that leverage CDAO's and DoD's enterprise data, analytics, and/or AI capabilities to enhance decision-making processes and practices for any DoD customers(s), as well as provide the data engineering, data analytics tools, shared services, and infrastructure for the CDAO Advana program at the platform layer and below.

Requirements may be fulfilled with commercial and Commercial-Off-the-Shelf (COTS) items not otherwise available through DoD sources of supply, government-off-the-shelf (GOTS), non-developmental items (NDI), and/or modified COTS in accordance with the terms of individual TO/DOs that originate from this IDIQ.

Requirements for specific products and/or services and Contract Data Requirements Lists (CDRL) will be defined in the requirements documents included in each order. These orders may include all or a portion of the requirements within this General Requirements work statement. The services outlined in this General Requirements work statement may support all aspects of identified or potential military, national security-related, and dual-use applications of related technologies and methods, as well as the development of tools, processes, and techniques that enhance the mission of the DoD.

DOs/TOs resulting from this IDIQ General Requirements work statement may involve multi-year performance; may involve work for any DoD customer(s); may require performance at multiple worldwide locations, to include performance outside the United States of America; may require access to controlled locations and facilities; and may require personnel clearances up to Secret, Top Secret, Top Secret Sensitive Compartmented Information, and/or Special Access Programs.

2.2 Ability To Statements

This IDIQ will enable DoD to accelerate decision advantage by partnering with digital capability providers that can meet some or all of the following "Ability To" statements to support requirements across a broad DoD-wide data management, analytics, and artificial intelligence ecosystem:

2.2.1. Systems Management, Architecture, and Engineering

The Contractor shall provide comprehensive system management, architecture, and/or engineering services to conceive, plan, acquire, manage, architect, engineer, document, and/or maintain the system management, architecture, and engineering products, artifacts, and resources required for systems, platforms, and solutions, by performing and/or delivering:

- Platform or System Architectures
- Systems Engineering
- Technology Standards, Interfaces, and Application Program Interfaces (API)
- Process Engineering
- Change Management
- Capacity Management
- Cloud Engineering
- Network Engineering
- Cross Domain Engineering
- Platform and System Audit

2.2.2. Software Engineering

The Contractor shall provide lifecycle software development to scope, plan, manage, design, develop, integrate, package, test, authorize, and/or deliver software, by performing and/or delivering:

- Software Design and Development
- Development, Security, and Operations (DevSecOps)
- Agile Software Management
- Configuration Management
- Commercial/Open-Source Tool Integration
- Cloud Native Service Integration
- Robotic Process Automation (RPA)
- Software Testing, Evaluation, and Validation
- Software Release and Deployment Management
- Software Reliability Engineering

2.2.3. Data Engineering

The Contractor shall provide comprehensive data engineering to scope, plan, manage, design, develop, integrate, package, test, authorize, deliver, operate, and/or maintain data pipelines and/or data solutions for organizations, and/or communities, by performing and/or delivering:

- Enterprise Data Operations
- Extraction, Transformation, and Load (ETL)
- Data Architectures
- Metadata Standardization
- Data Acquisition
- Data Ingest
- Data Engineering
- Data Tagging
- Data Quality Assurance
- Data Security
- Data Governance

2.2.4. Data Analytics

The Contractor shall provide comprehensive analytics services to scope, plan, manage, design, develop, integrate, package, test, authorize, deliver, operate, and/or maintain custom analytic solutions for organizations and/or communities, by performing and/or delivering:

- Enterprise Analytic Solutions and Integration
- Analytic Design and Development
- Analytic Testing, Evaluation, and Validation
- Analytic Operations
- Product Management
- Data Visualization
- Standardized Analytic Libraries and Templates

- Custom Analytic Tool Development

2.2.5. Artificial Intelligence/Machine Learning (AI/ML)

The Contractor shall provide comprehensive AI/ML engineering to scope, plan, manage, design, develop, train, validate, integrate, package, test, authorize, deliver, operate, and/or maintain AI/ML solutions for individual customers, organizations, and/or communities, by performing and/or delivering:

- AI/ML Design and Development
- AI/ML Data Labeling
- AI/ML Pipelines
- AI/ML Training
- AI/ML Testing, Verification, and Validation
- AI/ML Integration
- AI/ML Operations
- Responsible and Ethical AI/ML
- Standardized AI/ML Libraries and Templates
- Foundational AI/ML Solutions

2.2.6. Cybersecurity

The Contractor shall provide cybersecurity engineering, risk management, and authorization support services to conceive, plan, build, validate, authorize, operate, and/or maintain the security controls, system authorizations, and runtime cyber defense processes for securing and protecting systems, platforms, and solutions, by performing and/or delivering:

- Cybersecurity Risk Management
- Cybersecurity Requirements
- Cybersecurity Architecture
- Cybersecurity Engineering
- Security Controls Design and Implementation
- Identity, Credential, and Access Management (ICAM)
- Zero Trust
- Cybersecurity Compliance Testing
- Continuous Monitoring
- Security Incident Management and Response
- Penetration Testing

2.2.7. Managed Services

The Contractor shall provide a full range of managed services to operate, defend, and/or maintain enterprise systems, platforms, and solutions, to include comprehensive customer and end user support to facilitate enterprise systems, platforms, and solutions access and effective use, by performing and/or delivering:

- Incident Management and Response.
- Managed Service Process Engineering
- System Operations
- Service Portfolio Management
- Service Desk Operations
- Service Level Agreements
- Procuring and Managing Licensed Software or Cloud Services
- Cloud Brokering
- Customer Resource Utilization Tracking and Billing
- User and Access Management
- System and Data Back Ups
- Continuity of Operations
- Event Management
- Problem Management
- Knowledge Management
- Training Materials

2.2.8. Workflow Modernization

The Contractor shall provide a full range of services to assist enterprise stakeholders, customers, users, and communities to become highly proficient data management, analytics, and/or AI practitioners, and to evolve, align, and optimize operations and practices to improve mission outcomes, by performing and/or delivering:

- Portfolio Management
- Standard Operating Procedures
- Strategic Communications
- Stakeholder Engagement
- Customer Relationship Management
- Demand Management
- Use Case Intake Operations
- Workspace Operations

3.0 Requirements

Other than CDRL A001, all required deliverables, milestones, and/or CDRLs will be tailored to and thoroughly identified in DOs/TOs issued under this IDIQ contract. Tasks outline in DOs/TOs issued from this IDIQ are required and may vary from contract to contract as they are wholly dependent upon the technologies and/or products being acquired at that time.

3.1 Analytics Application Development

The contractor shall deliver platform-agnostic (e.g., interoperable with DoD platforms other than Advana) analytics application development under this IDIQ. Analytics application tasks include, but are not limited to:

- Provide customer-focused agile teams with multidisciplinary skillsets across business domain challenges and leveraging use case teams comprised of skillsets such as: data scientists, software developers, production analysts, and software testers.
- Use best in class agile or other similar methodologies for application development, where the development is organized into one or more releases consisting of multiple sprints.
- Deliver use-case specific applications using enterprise tools and capabilities as well as custom software where required. Leverage enterprise CI/CD pipelines and processes to deploy software and integrate web application content into the CDAO Content Management System (CMS).
- Build web-apps and other containerized applications from scratch and deploy them on NIPR, SIPR, and/or JWICS, as required, covering the entire IT engineering lifecycle including requirements gathering, system design and development, installation, integration and testing, and sustainment.
- Develop use case and application-specific data products that follow all data mesh principles, policies, and procedures provided by CDAO.
- Optimize prototypes and convert proven ideas into robust capabilities for delivery.
- Deliver on-demand data science capability to allow DoD organizations to continuously and persistently use data science to positively impact the operating mission, leveraging a team comprised of both highly experienced data science experts and functional expertise with deep rooted knowledge of the business domain, mission space, and data.
- Obtain, integrate, clean, and prepare data for building customized analytic, AI, and decision products for CDAO customers.
- Explore, analyze, and summarize large, diverse datasets through multiple technologies and techniques to enable decision-making.
- Research, acquire, and apply data fusion methods and techniques that address analysis, and protection of personally identifiable information (PII) or protected health information (PHI) of DoD military and civilian personnel and military personnel dependents.
- Provide data model support for user-defined data structures and schemas.
- Create data products using a variety of API mechanisms (e.g. DoD, Advana and others) for internal and external application use.

- Coordinate with functional and technical stakeholders to define methods for enriching, aggregating, and exposing data in a curated form to support analytics at scale in support of use cases of various maturity levels.
- Leverage master data management tools and services for the development of products such as lookup tables, business glossaries, and data profile information.
- Deploy validated models into production to support the development of decision support tools, dashboards, workflows and use cases.
- Leverage user-centered design methods to provide support for User Interface/User Experience (UI/UX) software development efforts to design and create applications with User Centered Design (UCD) methodologies to develop the right solutions.
- Leverage automated DevSecOps solutions to design, build, and deliver customized solutions to DoD customers.
- Provide the ability to surge in/out Data Scientists, Data Engineers, and Functional SMEs to respond to an incident/world event. Requires flexibility on geographical location support and the potential for work outside of normal business hours.

3.2 Enterprise Architecture

The contractor shall perform Enterprise Architecture activities as required for designing and implementing systems, platforms, and solutions developed under this IDIQ. Enterprise Architecture tasks include, but are not limited to:

- Developing and preparing Enterprise Architectures for CDAO enterprise data, analytic, and AI/ML systems and platforms.
- Developing web-apps and other containerized applications from scratch and deploy them on NIPR/SIPR/JWICS as required (on requisite Gov systems) covering the entire IT engineering lifecycle including requirements gathering, system design and development, installation, integration and testing, and sustainment.
- Designing, preparing, and documenting network architectures, cloud architectures, system architectures, data, architectures, software architectures, test architectures, and cybersecurity architectures.
- Preparing Enterprise Architecture products and documents to support the authorization of CDAO enterprise data, analytic, and AI/ML systems and platforms.
- Developing and proposing technical standards and coming APIs for DoD data, analytic, and AI/ML systems and platforms.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.3 Systems Engineering

The contractor shall perform Systems Engineering activities required for scoping, designing, implementing, and securing systems, platforms, and solutions developed under this IDIQ. Systems Engineering task include, but are not limited to:

- Collecting, organizing, and maintaining requirements.
- Designing, preparing, and documenting systems engineering products.
- Designing, implementing, and operating system engineering processes and decision boards.
- Preparing and maintaining engineering roadmaps and schedules.
- Developing and preparing Systems Engineering alternatives and courses of action (COAs) to support major leadership decisions.
- Preparing cost, schedule, and risk estimates for change requests to CDAO system, platform, or solutions.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.4 DevSecOps Solutions and Services

The contractor shall provide DevSecOps Solutions and Services as required for automating all the software/system lifecycle of all systems, platforms, and solutions developed under this IDIQ. DevSecOps Solutions and Services tasks include, but are not limited to:

- Designing and implementing enterprise DevSecOps solutions for data, analytic, and AI systems, platforms, and solutions.
- Designing and implementing automated DevSecOps pipelines to support CDAO data, analytic, and AI software lifecycles.
- Identifying, recommending, and incorporating Government approved tools into automated DevSecOps pipelines.
- Designing, implementing, and operating DevSecOps solutions to support CDAO data, analytic, and AI software lifecycles.
- Designing, implementing, and operating DevSecOps processes to support CDAO data, analytic, and AI software lifecycles.
- Aligning and operating DevSecOps processes and operations with CDAO Change Management Control Board (CCB) and Engineering Control Board (ECB) activities.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.5 Software Development and Integration

The Contractor shall perform Software Development and Integration activities as required for designing, coding, and implementing systems, platforms, and solutions developed under this IDIQ. Software Development and Integration tasks include, but are not limited to:

- Designing, implementing, and operating modern agile software processes in support of CDAO system, platform, and solution implementation.
- Designing, building, securing, and testing software to implement CDAO system and platform user stories and requirements using Agile sprint cycles.
- Constructing user stories to guide the development of software for CDAO platforms, systems, and solutions.
- Integrating and securing commercial and open-source tools into CDAO systems and platforms as directed by the Government.
- Hardening and securing Virtual Machine Images and software containers in accordance with DoD cybersecurity standards.
- Designing, building, and testing software application program interfaces (API) for supporting machine-to-machine interactions with CDAO systems, platforms, and solution services.
- Designing, building, and testing user interface software for supporting user facing interactions with CDAO systems, platforms, and solutions.
- Designing, developing, and testing Infrastructure-as-Code (IaC) and Configuration-as-Code (CaC) for provisioning and configuring and CDAO platforms and systems.
- Participating in and supporting CDAO software-related processes including DevSecOps and CCB/ECB processes.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.6 Test, Evaluation, Verification, and Validation

The Contractor shall perform Test, Evaluation, Verification, and Validation activities as required for systems, platforms, and solutions developed under this IDIQ. Test, Evaluation, Verification, and Validation tasks include, but are not limited to:

- Designing, preparing, and documenting test plans and procedures.
- Planning and conducting independent tests and evaluations of CDAO system, platforms, and solutions.
- Designing and implementing automated test procedures for incorporation into CDAO DevSecOps automated test pipelines.
- Identifying, evaluating, and reporting on new test tools and technologies that may be applicable to CDAO data, analytic, and AI/ML test and evaluation activities.
- Planning and conducting independent verification and validation of analytic and AI/ML models.
- Planning and conducting ongoing testing, evaluation, verification, and validation operations as part of CDAO's continuous DevSecOps processes and Engineering Control Boards (ECBs).
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.7 Cybersecurity

The Contractor shall perform Cybersecurity activities as required for risk management, authorizing, securing, and defending systems, platforms, and solutions developed under this IDIQ. Cybersecurity tasks include, but are not limited to:

- Performing cybersecurity architecture and engineering.
- Providing personnel that are qualified to perform the functions of DoD Information System Security Managers (ISSMs) and that have all DoD mandated qualifications and certifications for performing ISSM functions.
- Defining, designing, implementing, testing, authorizing, and maintaining appropriate NIST security controls for CDAO systems, platforms, and solutions.
- Designing, developing, and continuously improving Zero Trust architectures and security controls for CDAO systems, platforms, and solutions.
- Generating, preparing, and maintaining IATT, ATO, and Change Request (CR) engineering artifacts and documents for CDAO systems, platforms, and solutions using the DoD Risk Management Process (RMF).
- Defining, developing, and integrating automated cybersecurity test procedures into DevSecOps testing pipelines for CDAO systems, platforms, and solutions.
- Preparing, implementing, and maintaining Cybersecurity Continuous Monitoring Plans and conducting cybersecurity continuous monitoring and defense operations for CDAO systems, platforms, and solutions.
- Preparing, implementing, and maintaining Security Incident Management Plans and conducting Security Incident Management operations for CDAO systems, platforms, and solutions in accordance with all DoD and Government cybersecurity regulations.
- Preparing and maintaining System Penetration Test Plans and conducting penetration testing on CDAO systems, platforms, and solutions.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.8 Operations and Maintenance

The Contractor shall perform Operations and Maintenance activities as required for deploying, operating, administering, and maintaining systems, platforms, and solutions developed under this IDIQ. System Operations and Maintenance tasks include, but are not limited to:

- Preparing, implementing, and maintaining System Operation Plans and Incident Management Plans and conducting the full Operations and Maintenance (O&M) lifecycle for CDAO systems, platforms, and solutions.
- Performing system administration and maintenance activities on CDAO systems, platforms, and solutions as required to keep them operational.
- Managing and maintaining cloud environments via Cloud Service Provider (CSP) provided cloud service management consoles.
- Continuously monitoring the CDAO systems, platforms, and solutions for Virtual Machine or Container failures and restarting and restoring them to normal operations when necessary.
- Collecting, analyzing, and reporting ongoing system operations and maintenance issues so that they may be corrected in future releases.
- Installing, configuring, and operating Government-specified automated tools to track network configuration; monitor status and performance; detect, diagnose, and resolve network problems; and project future capacity requirements.

- Preparing, implementing, and maintaining Backup and Recovery Plans and providing failure recovery support for CDAO systems, platforms, and solutions to ensure the ability to restore Advana Platform service when needed.
- Notifying users of system outages and establish/maintain a business process to ensure any system outages, scheduled or not, are known and conveyed to users in a timely manner.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.9 Enterprise Data Engineering and Operations

The Contractor shall perform Enterprise Data Engineering and Operations activities as required for acquiring, ingesting, aligning, cleaning, tagging, advertising, and sharing enterprise data for all DoD data sources addressed under this IDIQ. Enterprise Data Engineering and Operations tasks include, but are not limited to:

- Designing, implementing, and maintaining Enterprise Data Engineering and Operations Plans and processes.
- Defining, documenting, and maintaining technical standards and best practices for Enterprise Data Engineering and Operations.
- Negotiating and establishing data sharing agreements between DoD data providers and CDAO systems and platforms.
- Designing, implementing, testing, authorizing, and operating data ingest pipelines for continually importing DoD enterprise data into CDAO systems and platforms.
- Conducting DoD Enterprise Data Engineering and Operations to import DoD enterprise data into CDAO systems and platforms.
- Designing, implementing, testing, authorizing, and operating enterprise data tagging capabilities for enterprise data imported into CDAO systems and platforms.
- Designing, implementing, testing, authorizing, and operating enterprise data cleaning and quality control capabilities for enterprise data imported into CDAO systems and platforms.
- Implementing and operating enterprise data ingest monitoring mechanisms to proactively address any issues that may arise over time.
- Designing, implementing, testing, authorizing, and operating enterprise data discovery and sharing services/APIs to enable machine-to-machine capabilities.
- Designing, implementing, testing, authorizing, and operating data governance mechanisms that enable users to rapidly discover and access enterprise data using attribute-based access control.
- Developing and maintaining training and certification programs for data connection engineers that grants access and enables data sharing across CDAO and DoD systems and platforms.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.10 Governance

The Contractor shall perform Governance activities as required for acquiring, ingesting, aligning, cleaning, tagging, advertising, and sharing enterprise data for all DoD data sources addressed under this IDIQ. Governance tasks include, but are not limited to:

- Design, implement, and maintain policy-based governance mechanisms for managing the access and use of enterprise platform resources including cloud capacity, tools and services, pipelines, data, analytics, AI models, and visualization applications.

3.11 Information Technology (IT) Resource Acquisition and Management

The contractor shall assist the Government in assessing identifying, acquiring, and managing commercially procured IT resources including, but not limited to, software licenses, cloud capacity, and technical support. IT Resource Acquisition and Management tasks include, but are not limited to:

- Gathering and managing requirements for IT resource acquisition and management activities.
- Conducting technical reconnaissance of commercial and open-source IT products and services to identify capabilities of interest to the Government.
- Preparing Course of Action analyses for IT resource acquisitions to assist the Government in making IT tool, service, and cloud selections.
- Negotiating with commercial and open-source product vendors to obtain the best possible prices for the Government for IT resource purchases.
- Managing and maintaining configuration management of procured IT resources and services.
- Integrating IT resource management with CDAO processes and control boards.
- Preparing and maintaining predictions of future IT resource acquisitions based on CDAO and CDAO customer needs.

3.12 Product Management

The Contractor shall perform Product Management activities as required for products designed, developed, and/or deployed under this IDIQ. Product Management tasks include, but are not limited to:

- Conduct and execute a product operating model for the data products, analytic applications, and custom software from beginning of lifecycle to end. Identify the vision of a product(s), directs updates, and ensures the product(s) are filling customer needs until the product(s) are retired.
- Define key metrics for product success and build mechanisms to report those metrics to customers.
- Conduct continuous discovery and delivery of each product using modern product management principles and operating models.
- Work with cross-functional teams and stakeholders (e.g., engineering, design) to develop and pursue product strategy.
- Find ways to improve products through analysis, user adoption and use feedback.
- Monitor and measure product performance.

- Test and monitor new product features using modern GitOps pipelines where feasible and maintain agile practices in the discovery and delivery of such products.
- Monitor alternate products through market analysis and research.
- Maintain engineering, product management, and product design staff that are current on industry best practices and translate those into CDAO and DoD tools and capabilities where applicable.
- Design and staff a community support team to address intake, dedicated account manager(s), and requisite program management support and oversight for a continuum of individual builders all the way up to large functional activities.

3.13 Business Operations

The Contractor shall perform Business Operations required for accelerating adoption and implementation of data, analytic, and AI operational efficiencies under this IDIQ. Business Operation tasks include, but are not limited to:

- Establish, maintain, and continually improve a framework and process for accelerating user adoption, user proficiency, and user mission effectiveness within the Advana Platform.
- Build strategic communication initiatives developing communication materials and messaging to customers, users and stakeholders in support of a new operating model such as: available product and service offerings, mapping out user stories and journeys, graphically designed communications products in all formats with branding (e.g. online, written, slick sheets among others) video/dynamic products and technical engineering products. All products should align to personas and stakeholder engagement goals and expectations that are continuously reviewed, revised, and re-implemented based on customer needs and current CDAO service offerings.
- Apply Information Technology Infrastructure Library (ITIL) framework practices to accelerate implementation of a new CDAO operating model focused on enabling Mission Analytics scale for DoD to include elements such as but not limited to stakeholder outreach and integration, change management, measurement and reporting, customer success, portfolio management, product, data and service catalog
- Sets the vision of a customer-focused strategy, directs updates, and ensures service-offerings are filling customer requirements.
- Build a knowledge management system to capture the creation, sharing, usage, and management of knowledge and information about CDAO and its service offerings. This should include written products, graphically designed products, video/dynamic products and technical engineering products.

3.14 Program Management

The Contractor shall perform Program Management activities, as required, for planning, coordination, organization, and execution of all program management related tasks to include, but not limited to:

- Development, documentation, reporting of all program management processes, products, and artifacts.
- Financial and contractual performance documentation and reporting.
- Configuration management and data management, including risks and issues management.
- Cost and schedule tracking and reporting; subcontract management and reporting.
- Prepare and maintain program roadmaps and an Integrated Master Schedule (IMS), overseeing the execution of program activities to ensure schedules are met. This IMS should nest with and be traceable to the current DoD Strategic Management Plan, incorporate all DoD Senior Leader Decision Support Framework governance fora, and align with the DoD Planning, Programming, Budgeting, and Execution (PPBE) system.
- Implement an Agile software management process across Advana and host a viable Agile Community of Practice for the promulgation of consistent practices in Objective and Key Results (OKR) guidance, Strategic Roadmap development, Increment Planning, and daily task management.

3.15 Customer Support and Service Desk

The Contractor shall perform Customer Support and Service Desk activities as required for assisting customers and users that utilize systems, platforms, and solutions developed under this IDIQ. Customer Support and Service Desk tasks include, but are not limited to:

- Developing, building, and maintaining Service Desk Operations Plans and associated processes.
- Designing, implementing, and operating Service Desk(s) for providing Tier 0, 1, 2, and/or 3 customer/user support for CDAO systems, platforms, and solutions.
- Supporting rapid service requests for Very Important Persons (VIPs) including General Officers, Flag Officers, Senior Executives (SESs), and certain senior level political appointees.
- Performing account maintenance and setup activities, including creating, modifying, and/or deleting user accounts in support of account maintenance policies and Standard Operating Procedures (SOPs).
- Preparing and maintaining Service Desk performance metrics.
- Designing, building, and maintaining Service Desk Queue Management plans and associated processes.
- Reviewing and evaluating Service Desk process performance and conducting root cause analysis to identify, address, and remedy Service Desk performance issues and resolve negative trends.
- Conducting regular communications with customers/users to keep them informed of System issues, outages – both planned and unplanned.

- Designing, preparing, validating, and promulgating Service Desk training materials and documentation that assist customer and users in accessing and using CDAO systems, platforms, and solutions.
- Implementing and maintaining Service Desk SOPs and Service Desk Playbook for Tier 1 and Tier 2 to address common procedures and problems.
- Collecting, archiving, and maintaining Service Desk logs and operations data required to support CDAO and DoD system audits.
- Conducting and reviewing customer/user feedback to continually improve quality and breadth of Service Desk offerings.
- Performing additional tasks as defined in individual TO/DOs executed from this IDIQ.

3.16 Data Engineering and Data Science Solutions

The Contractor shall assist customers in defining, scoping, planning, implementing, testing, authorizing, and delivering Data Engineering and Data Science Solutions developed under this IDIQ.

3.17 Artificial Intelligence and Machine Learning Solutions

The Contractor shall assist customers in defining, scoping, planning, implementing, testing, authorizing, and delivering Artificial Intelligence and Machine Learning Solutions developed under this IDIQ.

3.18 Robotic Process Automation

The Contractor shall assist customers in defining, scoping, planning, implementing, testing, authorizing, deploying, managing, and monitoring cloud-based Robotic Process Automation (RPA) solutions to accomplish workflow optimization under this IDIQ.

4.0 Security

The Contractor personnel may be required to access a federal government/military facility on a temporary basis to deliver and/or maintenance equipment. Access to federal facilities may require the Contractor personnel to submit to a criminal background check which may include an FBI fingerprint check. The Contractor shall comply with any additional local requirements specific to the facility location of access.

For Contractor personnel whom will require military installation access and/or privilege access to DoD information technology systems: the Contractor shall ensure all personnel, who are authorized users of an information technology system, hold a favorably completed Tier-3 (T3) investigation, or National Agency Check with law and credit (NACLC), or Access National Agency Check and Inquiries (ANACI) with collateral level access and receive a current periodic reinvestigation in accordance with DCSA guideline for access levels. The Contractor shall ensure applicable Contractor personnel have security clearances at the appropriate level for proper accomplishment of contract/order requirements.

4.1 Security Management

The Contractor shall comply with the security requirements specified in each DO/TO issued from this IDIQ. The Contractor shall flow down the security requirements to subcontractors as applicable. All resources (e.g., publication/instructions) provided by the Government to assist the Contractor in the performance of their contract shall be surrendered at the end of the contract period of performance or upon Government request.

4.2 Operations Security

The Contractor shall ensure operations security (OPSEC) is incorporated into the appropriate area of the contract IAW DoD Directive 5205.02M, DoD Operations Security Program Manual. The contractor shall flow down all OPSEC requirements to subcontractors that handle Critical Information (CI). CI is defined as specific facts (or evidence) about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishments.

4.3 Controlled Unclassified Information

The Contractor shall ensure all personnel who are authorized users of an information technology system with "no privileged access" (IT Level III) duties hold a favorably completed Tier 1 investigation; IT Level II ("privileged access") duties hold a favorably completed Tier 3 investigation; and IT Level I ("privileged access") duties hold a favorably completed Tier 5 investigation and receive a periodic reinvestigation every 5 years.

Additionally, the Contractor shall comply with DoD standards for storing, processing, marking, and handling unclassified and/or Controlled Unclassified Information (CUI) and systems pursuant to FAR 52.204-21 and DFARS 252.204-7012. The Contractor shall monitor CUI aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information.

4.4 Personnel Security

The Contractor shall ensure applicable contractor personnel have security clearances at the appropriate level for proper accomplishment of DO/TO requirements. The security clearance shall be obtained in accordance with the DO/TO. Contractor personnel whose clearances have been suspended or revoked shall immediately be denied access to classified information and/or CUI and classified items.

4.5 Security Incidents and Violations

The Contractor shall notify the Government Contracting Activity and the Government Security Manager within 48 hours of any incident involving the actual or suspected compromise/loss of classified information to enable the Government to conduct immediate assessments of potential impact pending formal inquiry/investigation. Actual or suspected compromise of Covered Defense Information will be reported IAW DFARS Clause 252.204-7012.

5.0 Travel

The Contractor may be required to travel in support of the IDIQ DO/TOs. For example, the Government may require the Contractor to travel, either domestic or foreign, to seminars, conferences, workshops, meetings, events, commercial vendor sites, test facilities, military installations, and/or specialized to perform the objectives of an awarded DO/TO. When necessary, travel requirements will be outlined in each DO/TO.

6.0 Property, Equipment, Facilities, and Information

Government furnished property, equipment, facilities, and/or information may be provided under certain projects and will be specified at the DO/TO level, as appropriate.

7.0 Small Business Subcontractor Reporting

IAW basic contract CDRL A001 – Small Business Subcontractor Report, the Contractor shall report small business subcontracting activity for awarded DO/TOs under the Unrestricted (UR) Pool. This CDRL applies to both small businesses and other than small businesses for awarded DO/TOs under the UR Pool.

8.0 Performance Management

8.1 Contractor Performance Assessment Report

The Government does not intend to evaluate the basic IDIQ contracts within the Contractor Performance Assessment Reporting System (CPARS). When a placed DO/TO exceeds the threshold specified in FAR Subpart 42.15, the Assessing Official at the contracting or requiring activity for that DO/TO is responsible for completing a separate evaluation in CPARS.

8.2 Dormant Status

IAW section H.5 of the basic contract, the AAMAC Contracting Officer may, if determined necessary, remove an AAMAC contractor from the Unrestricted (UR) Pool, Small Business (SB) Pool, and/or SB Pool Reserve(s) and place them in a Dormant Status. When placed in a Dormant Status, the Contractor will be ineligible to compete for new delivery orders or task orders issued under the UR Pool, SB Pool, and/or SB Pool Reserve(s). However, Contractors placed in Dormant Status shall continue performance on all awarded delivery orders or task orders, to include exercised options and/or modifications.

For example, if an AAMAC contractor was required to have an acceptable subcontracting plan (SBSP) or commercial plan (CP) to receive an IDIQ contract and does not timely respond to the AAMAC Contracting Officer's deadline to submit a post-award SBSP or CP update pursuant to Section H.1, that contractor may be placed into a Dormant Status. This is just one example and does not represent all potential circumstances that may warrant placing an AAMAC contractor into Dormant Status.

Dormant Status is not a Debarment, Suspension, or Ineligibility as defined in FAR Subpart 9.4. Additionally, it is not a Termination as defined in FAR Part 49. Rather, Dormant Status is a condition that applies to this AAMAC contract only.

Grounds for placing an AAMAC contractor into Dormant Status include, but are not limited to:
(a) Trends or patterns of behavior associated with the failure to meet the deliverables or comply with the contract.
(b) For the SB Pool, the AAMAC contractor no longer represents as a small business under the NAICS code for this acquisition.
(c) Within a SB Pool Reserve, the AAMAC contractor no longer represents as the type of small business concern qualifying for the reserve (e.g., an AAMAC contractor within the 8(a) Program Reserve graduates the 8(a) Business Development program.

The AAMAC Contracting Officer will place a contractor into Dormant Status only after consideration of the situation and, in event of condition (a) or substantially similar to condition (a), when attempt(s) to collaborate with the contractor and resolve the issues are unsuccessful. For (b), placement into Dormant Status under the SB Pool does not mean that the AAMAC Contractor will be placed into Dormant Status under the UR Pool. For (c), placement into Dormant Status under an SB Pool Reserve does not mean that the AAMAC Contractor will be placed into Dormant Status in the UR Pool, SB Pool, or any other applicable SB Pool Reserve.