Army Leader Dashboard

DRAFT Statement of Work

20 April 2018

This page intentionally left blank

Table of Contents

1. STATEMENT OF WORK – Army Leader Dashboard

1.1 Problem:

The Army lacks visibility into the vast amount of data, dispersed across the Army enterprise.

The Army requires a big data management solution and a tailorable solution that integrates, analyzes, and visualizes information from multiple disparate data sources, both classified and unclassified. The solution should present information in a way that is immediately understandable and actionable for an everyday end-user. The solution should be capable of integrating both current and historical structured/unstructured datasets, perform predictive analytics and forecasting. The product(s) shall be commercially available now.

1.2 Purpose:

This project will take advantage of Commercially Available software solution(s) to configure the prototype(s) as an Army Leader Dashboard (ALD) to allow user assessment of the initial capability for a decision-making, reporting and visualization capability. The dashboard shall enable Army Senior leaders and leaders at designated levels to easily navigate through information from multiple Army Authoritative Data Sources (ADS's) in order to capture information to produce predictive analytics and facilitate real-time or near real-time decision making. This effort shall include an Agile Methodology for data integration and visualization responding to Senior Army Leader input. The solution shall have proven maturity to permit expansion of the user base and long term sustainment.

1.3 Scope:

The Solution must provide the ability to visualize the current and future state of the Army based on data generated by the thousands of systems that support the Army's execution of its primary functions under Title 10 and Title 32, United States Code (USC) to organize, man, train, equip, and sustain forces. The solution must be able to collect, catalogue, manage, integrate, aggregate, analyze and visualize data from these disparate systems and other external data sources.

The solution must have the ability to scale data aggregation to thousands of current/legacy Authoritative Data Sources (ADS) and millions of data points (both structured and unstructured), and be able to secure data at the most granular level and authenticate by system and user. Additionally the solution should account for and include all required integration to ensure the end-solution is deliverable. The integration should include but is not limited to data ingestion, management, analytics, cleansing and visualization and geospatial services. The visualization output should provide minimally-trained senior leaders an intuitive and configurable dashboard-style interface to visualize and present information in ways that are immediately understandable and actionable. Additionally, the solution shall demonstrate the ability to support real-time/near real-time senior leader decision making.

The solution must be capable of achieving Federal security compliance standards. The product shall be commercially available, demonstrable and take into consideration leveraging existing Army software investments to the greatest extent possible.

For the ALD prototype project, the term "commercially available" is a compilation of three definitions which can be found in file name App_001:

"Commercial component" means any component that is a commercial item.

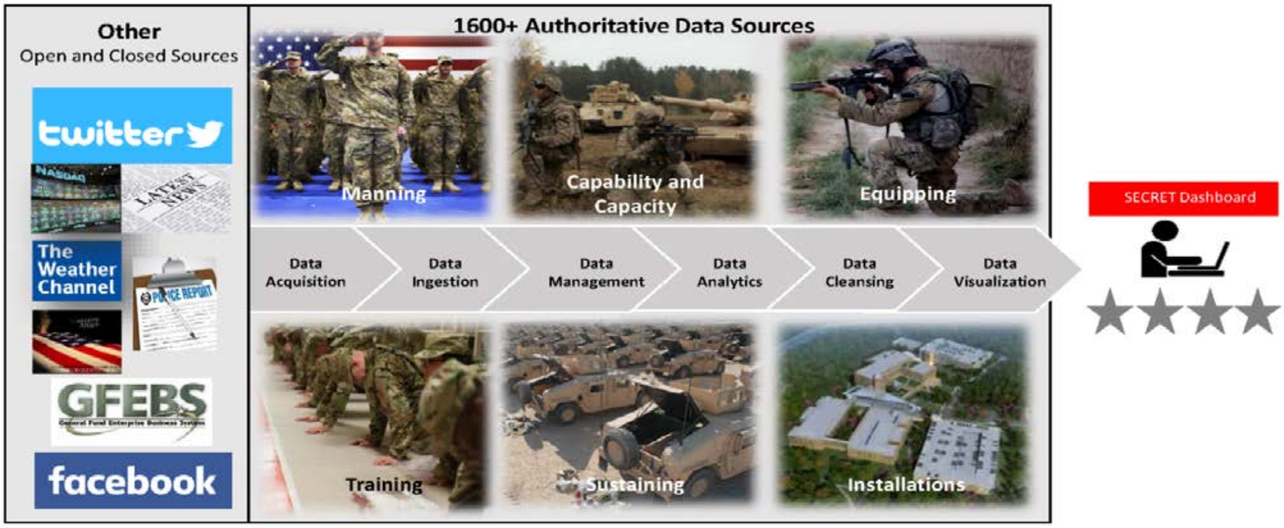
“Commercial computer software” means any computer software that is a commercial item.

“Commercial item” means any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes, and—

(1) Has been sold, leased, or licensed to the general public; or

(2) Has been offered for sale, lease, or license to the general public

Figure 1 ALD Operational View of Capability



1.4 User Base:

During Phase 1, the ALD will be provided first to one (1) Army Senior Leader and up to 20 designated alternates with a scalable solution for the purpose of continuous prototype assessment. During Phase 2, the scalable solution will be subsequently released to the 150 designated Army Leaders (users) at the division, brigade, battalion, and below levels across the entire Army.

2.0 PROTOTYPE PHASES AND ASSESSMENT

This project will use a phased approach as outlined below:

2.1 Phase 1: (up to 120 Calendar Days) Day 1 is date of agreement award.

2.1.1 **Task 1.** The Contractor shall configure, integrate, demonstrate and release / provide access to the ALD within five (5) business days after award to one (1) Senior Leader (user). At the initial five (5) day delivery, the prototype is expected to be a function of the capabilities of the offerors solution with the static data provided. Within thirty (30) days after award, the Solution shall be on the Army NIPR and SIPR Network(s) and available to the Senior Leader and up to twenty (20) designated alternates at Headquarters, Department of the Army (HQDA). During this phase, the Contractor shall initiates the development and integration of designated Interfaces and/or Application Program Interfaces (APIs).

2.1.2 **Task 2.** The Contractor shall conduct a study and analysis and submit a written report of the Army Authoritative Data sets beyond those identified in Phase 1 and Phase 2. The report shall provide an assessment of the number, size and frequency of data feed updates with a recommendation of priority (1 – N) for interfaces / connections. Additionally, the Contractor shall assess and report on how data is currently managed and recommend a strategy for enhancing data usability and information quality to include data cleansing and correcting. (Technical Report–Study/Services, DI-MISC-80508B)

2.1.3 Completion of this phase is up to 120 (Calendar days). Upward Invitation to Phase 2 will be based on successful completion of Tasks 1 and 2.

2.2 **Phase 2: (up to 245 Calendar Days from the start of phase 2)** The Tasks will be defined by the results of the Phase 1 Task 2 Studies and Analysis, and an updated Statement of work will be released. The Government anticipates Contractor Tasks shall include: continuation of configurations, delivery of solution on a desktop, laptop, tablet, and mobile device, hosting of the enduring solution, additional 25 ADS's, development and integration of additional APIs and/or designated Interfaces. The Contractor shall be prepared to scale the ALD to an additional 150 designated Army Leaders (users) at the division, brigade, battalion and below levels across the entire Army.

2.2.1 Completion of this Phase is up to day 245 (Calendar days) from start of phase 2.

3.0 OVERALL TECHNICAL REQUIREMENTS

The following are minimum requirements that will be included in the prototype:

3.1 Data Integration:

3.1.1 The Contractor shall deliver a commercial data management solution that acquires data from numerous unclassified and classified authoritative data sources in an automated manner that minimizes or eliminates the requirement for manual intervention during data acquisition and enables information management.

3.1.2 The data must be protected in accordance with applicable laws, regulations and policies governing Personally Identifiable Information (PII), Protected Health Information (PHI) and protection of the solution will be capable of:

3.1.3 Organizing and integrating data on NIPRNet and SIPRNet into a SIPRNet-hosted solution.

3.1.4 Data-agnostic data integration, including structured, unstructured, and semi-structured data integration capabilities at terabyte scale.

3.1.5 Data "pull" jobs through a RESTful web API or direct connections that refresh data and can be run manually or on a schedule.

3.2 Analytics and Visualization:

The Contractor shall deliver a configurable NIPRNet and SIPRNet solution(s) that:

3.2.1 Integrates, analyzes, and visualizes information in real-time/near real-time (within 24 hours of data updates) from multiple disparate data sources, both private and public.

3.2.2 Presents a broad and immediate awareness of actual or predicted Army status

3.2.3 Provides a solution that enables access and/or launches access through all modern Army approved (Classified and Unclassified) Army devices (desktop, laptop, tablet and mobile)

3.2.4 Presents information that is immediately understandable and actionable to users

3.2.5 Intuitive, interactive, top-down, large-scale data exploration application to allow nontechnical users to interactively explore massive-scale data in a drill-down, point-and-click application and filter billions of pieces of data into a digestible set of useful information.

3.2.6 Provides user defined alert(s) and ability to setup and tailor an alert "Ticker Tape" text banner

3.2.7 Provides plaintext search capability across all data

3.2.8 Provides ability to filter, receive/view alert(s) and share information with other users

3.2.9 Processes and displays all current data and available historic Army data as needed in order to provide future predictive analytics (5, 10, 20 + years into the future). The data sets are generated by approximately 4,000 systems registered in the Army Portfolio Management System of which 700 are registered business systems

3.3 Security and Infrastructure:

The Contractor shall deliver a configurable solution that provides:

3.3.1 Role-based access controls that are assignable to individual users or groups of users and are securely stored in lists, which can be updated at any time.

3.3.2 Multi Factor (Two-Factor) Authentication (e.g., enterprise LDAP, X.509 PKI, Active Directory, etc.) as well as Single Sign-On (SSO) capabilities using the Army's Identity and Access Management (IdAM) capability, Enterprise Access Management Service – Army (EAMS-A).

3.3.3 Protect data at rest and in transit using Federal Information Processing Standards (FIPS) 140-2 approved and validated algorithms for encryption, hashing, and signing (e.g., full disk encryption, Kerberos)

3.3.4 The ability to achieve an Interim Authority to Test (IATT) on DOD NIPRNet and SIPRNet for the duration of the prototype effort.

3.3.5 That meets or has the ability to meet the DOD Risk Management Framework (RMF) accreditation requirements for an Authorization to Operate (ATO) on DOD NIPRNet and SIPRNet. (DOD Risk Management Framework (RMF) Package Deliverables, DI-MGMT-82001)

3.3.6 That is capable of delivering integrated classified and unclassified content to SIPRNet users, and enable the Government to pass data and insights from an unclassified solution to a classified solution.

4.0 REGULATIONS AND POLICIES FOR REFERENCE

- **Army Regulation 220-1, Army Unit Status Reporting and Force Registration – Consolidated Policies, dated 15 April 2010**. This regulation consolidates into one authoritative publication Army policy for readiness status reporting for force registration. Also, it implements Chairman of the Joint Chiefs of Staff Instruction 3401.02 A, Chairman of the Joint Chiefs of Staff Manual 3150.02 A, DODD 6025.19, DODD 7730.65, and DODD 8500.1. Available at: http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/r220_1.pdf

- **Army Regulation 5-1, Management of Army Business Operations, dated 12 November 2015.** This regulation covers the management of Army business operations, the governance of the Army's Business Mission Area (BMA), and the sustainment of the Army's Business Systems (ABS) Architecture. Army business operations are those activities that enable the Army to execute effectively and efficiently its 10 USC primary functions to organize, man, train, equip, and sustain forces. Available at: http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/r5_1.pdf

- **Army Regulation 25–2, Information Assurance, dated 23 March 2009.** This regulation provides Information Assurance policy, mandates, roles, responsibilities, and procedures for implementing the Army Information Assurance

Program, consistent with today's technological advancements for achieving acceptable levels of security in engineering, implementation, operation, and maintenance for information systems connecting to or crossing and U.S. Army managed networks. Available at:
https://ia.signal.army.mil/docs/AR25-2.pdf

- **Risk Management Framework (RMF) for DoD Information Technology (IT), dated 24 May 2016.** This document reissues and renames DoD Instruction (DoDI) 8510.01, Implements References by establishing the RMF (Risk Management Framework) for DoD IT (Information Technology) establishes associated cybersecurity policy, and assigns responsibilities for executing and maintaining the RMF. Available at: https://www.hsdl.org/?view&did=793050

- **Department of Army Pamphlet 220-1 Defense Readiness Reporting System–Army Procedures, dated: 16 November 2011**. This pamphlet consolidates and updates the basic processes and general procedures for preparing, reviewing, and submitting the commander's unit status report and for accomplishing force registration actions. Available at:
http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/p220_1.pdf

- **Army Regulation 525-30 Army Strategic Readiness, dated: 3 June 2014.** This regulation prescribes the purpose, policies, procedures, and responsibilities for planning, preparing, executing, and assessing Army Strategic Readiness. Available at: http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/r525_30.pdf

- **Department of Army Pamphlet 525-30 Army Strategic Readiness Assessment Procedures, dated: 9 June 2015.** This pamphlet explains and documents the basic Army strategic readiness assessment processes and general reporting procedures used in determining, analyzing, assessing, and reporting Army Strategic Readiness in accordance with the three Joint Staff Criteria (Joint Capability Assessments, Army Plan Assessment, and Readiness Deficiencies) and six Army Strategic Readiness Tenets (Manning, Equipping, Sustaining, Training, Installations, and Capacity and Capability). Available at:
http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/p525_30.pdf

- **Army Information Architecture, Version 4.1, dated: 5 June 2015.** The Army Information Architecture (AIA), provides the design and development guidance needed by Army personnel, from Communities of Interest (COIs) to Program Managers (PMs) to developers, to create information systems that meet DoD and Army net-centricity and information sharing objectives. Available at:
http://ciog6.army.mil/

- **Army Data Strategy, Version 1.0, dated: February 2016.** Information Architecture Division, Army Architecture Integration Center, HQDA CIO/G-6. This document provides the basic Army strategic plan for data management and general governance procedures that impact the ALD Authoritative Data Sources. Available at:
http://ciog6.army.mil/Portals/1/Home/Tabs/Strategy/20160303_Army_Data_Strategy_2016.pdf

- **Defense Logistics Agency (DLA) Document Services, Acquisition Streamlining and Standardization Information System (ASSIST).** Managed by DLA Document Services, Philadelphia, ASSIST provides free access to Defense Standardization Program (DSP) technical documents that have been cleared for public release to include the Data Item Descriptions (DID) formats for the ALD contract deliverables. Quick Search available at: http://quicksearch.dla.mil/qsSearch.aspx

5.0 GENERAL REQUIREMENTS

5.1 Security:

5.1.1 The highest level of classification for this effort is SECRET. The Contractor shall comply with the Department of Defense Contract Security Classification Specification, DD Form 254, which required a Facility Clearance of Secret and designated personnel to possess a Secret Clearance. The Government will sponsor the Interim and Final Clearances as required.

5.1.2 The Government will sponsor designated Contractor personnel for Common Access Card (CAC) identifications and SIPR tokens. Those designated personnel will be required to complete the Government provided on-line annual security training for: a) Level 1 Anit-Terrorism, b) DoD Cyber Awareness Challenge Exam, and c) (sign) the DoD Acceptable Use Policy (for accessing a U.S. Government (USG) information system.

5.1.3 The Contractor shall establish control, procedures and training in order to properly secure Government data from unauthorized access or release providing Confidentiality. The Contractor will also limit options for unauthorized modifications providing data Integrity. Finally, the Contractor will maximize opportunities to provide uninterrupted access to dashboard products providing data Availability. A formal determination of Confidentially-Integrity-Availability (C-I-A) levels will be determined by the Government effecting the number of RMF Security Controls requiring assessment.

5.1.4 The Contractor shall protect access and release of Personally Identifiable Information (PII) and Personal Health Information (PHI). All Contractor personnel with access to the ALD Solution and the PII / PHI data shall complete all required annual Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) training conducted online through Army Records Management & Declassification Agency (RMDA) https://www.rmda.army.mil/privacy/RMDA-PO-Training.html to meet the above requirements.

5.1.5 The Contractor shall provide a solution which meets the Army classification requirements of Army readiness data according to Army Regulation (AR) 220-1.

5.2 Systems Engineering Management:

The Contractor should employ industry and DoD best practices for analysis, configuration, design, development, deployment and support of the Army Leader's Dashboard prototype.

5.2.1 The Contractor shall comply with applicable industry standards used in their systems engineering processes. The approach shall align to the requirements of the 2010 National Defense Authorization Act, Section 804 "Implementation of New Acquisition Process for Information Technology Systems", specifically, the approach shall include:

- early and continual involvement of the user;
- multiple, rapidly executed increments or releases of capability;
- early, successive prototyping to support an evolutionary approach; and

- a modular, open-systems approach

The systems engineering processes should include:

- Flexibility: tailoring program strategies and oversight
- Responsiveness: rapid integration of advanced technologies
- Innovation: adapt practices that reduce cost and cycle time
- Discipline: use of program baseline parameters as control objectives
- Effective Management: decentralization to the extent practicable

5.3 **Program Management:** The Contractor shall provide the overall management and administrative effort for the planning, organizing, staffing, directing, and controlling the tasks, activities and approval actions necessary to ensure that the ALD prototype is delivered on-time and meets the expectations of Army senior leaders.

5.4 **Data:** All Contractors that have access to the data provided for this effort shall adhere to all Data Usage Agreements, which can be found in file name APP_002. The Government intends to establish working groups with the various functional data owners.

5.5 **System Data Usage:** The solution shall not capture, maintain, scan, index, share or use data stored or transmitted by the system for any non-authorized activity or non-government purpose. The solution will include a specific process for handling spillage that ensures compliance with DoD requirements, including Army Spillage Best Business Practices (BBP), National Institute of Standards and Technology (NIST) Special Pub 800-88, DoDM 5200.01 Volumes 1 - 3, and DoD 5220.22-M. (DoDM 5200.01 Vol 3, February 24, 2012, Enclosure 6, Appendix 1 Report of Security Incident Inquiry or Investigation & Appendix 2 DoJ Media Leak Questionnaire)

5.5.1 System Records Management. All Government records processed, retrieved or displayed by the dashboard solution shall be maintained in compliance with the requirements of the Federal Records Act, 44 USC Chap. 33, the E Government Act of 2002, 44 U.S.C. 101, and the implementing regulations issued by the National Archives and Records Administration (NARA) at 36 CFR 1200 et seq. In addition to the Federal requirements for records management, Department of Defense Directive Number 5015.2.

5.5.2 Dashboard Technical Publications. As required by the Government, the Contractor shall provide the technical data needed to support the hosting and operation of the ALD solution. (e.g. identification of required Ports, Protocols and Services, firewall rules, power, signal, floor space, etc.)

5.5.3 Dashboard Support Data. The Contractor shall document and store in a data repository the data needed to support the provisioning process (i.e. preparing and equipping the dashboard to allow it to provide (new) services to its users). The Contractor shall document and store in a data repository the data needed to support transition of the prototype to production.

5.5.4 Prototype User Assessment Support: Provide services to support the Army's Senior Leader and Global Usability Assessment with support via solution experts. During the Usability Assessment, Government business hours/days, and on-call as needed, the Solution Experts shall be stationed in close proximity of the Pentagon Department of Army Headquarters to permit responses with an on-site representative (arrive at designated Army office within :120 minutes) to provide one-on-one support to Senior Leader users.

5.6 **Hosting:** The Hosting of the ALD solution will be managed by the Project Phase.

5.6.1 Hosting for Phase 1. The Government will provide a NIPRNet and SIPRNet hosting facility to support the development, test and demonstration of the ALD based on Infrastructure as a service. The Government anticipates that each Contractor will be provided a virtual machine environment on NIPRNet and SIPRNet.

5.6.1.1 The Contractor shall meet one of the following hosting options (a), (b) or (c):

(a) The Contractor shall install, configure and sustain a prototype Army Leader Dashboard software capability onto an Army provided infrastructure solution. The ALD will need to be able to receive data from a Secure File Transfer Protocol (SFTP) server to support initial data transfers from data providers. The hosting will be at Acquisition Logistics Technology Enterprise Systems and Services (ALTESS) Government Facility for the purpose of continuous prototype assessment. The hosting facility will provide access to both the Non-Secure Internet Protocol Router Network (NIPRNet) and the Secure Internet Protocol Router Network (SIPRNet). The Contractor support will include the capability to leverage an Army-provided Cross Domain Solution (CDS).

If the Contractor's solution requires custom hardware, ALTESS will provide data center rack space, power and cooling. All equipment shall be racked within the provided racks to allow the placement to be anywhere ALTESS deems appropriate based on the interfacing requirements. Contractor provided equipment must be able to fit within facility provided APC racks that accommodate vendor-neutral mounting for guaranteed compatibility with all EIA-310 compliant 19" equipment. This configuration is powered by APC Metered Rack Power Distribution Units (PDUs) provided with IEC 320 C19/IEC 320 C13 connections. The data center will provide network connectivity and cabling to a DoD DMZ security stack (firewalls, load balancer, reverse proxy). ALTESS will provide power, signal and rack space.

Contractor equipment hosted at ALTESS that processes sensitive, controlled unclassified information (CUI) will be sanitized in accordance with ALTESS "Media Sanitation Material Destruction SOP". Contractor equipment hosted at ALTESS that processes classified information will be destroyed in accordance with AR 380-5, Ch.3 Section 5. Material containing volatile information (classified or unclassified) identified by the client will be purged/sanitized and or destroyed once it is no longer needed or functioning.

(b) The Contractor shall deliver, install and configure a prototype Army Leader Dashboard solution which will be able to meet Army specific accreditation requirements (available upon request) and hosted within a DoD NIPRNet/SIPRNet hosting site. The ALD solution will need to be easily scalable to meet immediate requirement demands.

(c) The Contractor shall provide a hosting facility where the prototype Army Leader Dashboard solution shall be delivered, installed, configured and supported. The Contractor's hosting facility shall meet or meets or has the ability to meet DoD Security requirements impact level four (4) for the unclassified data and impact level six (6) for the classified data (available upon request). The solution will need to be easily scalable to meet immediate requirement demands. Offerors proposing their own hosting facility would be responsible for moving data from NIPRNet to SIPRNet.

5.6.2 Hosting for Phase 2. The Government is looking to industry to propose the best hosting environment for phase 2 and for the enduring solution(s) which meets DoD Security requirements and/ applicable impact levels.

5.6.3 System Application Program Interfaces (API(s)) and Interface Development. The ALD baseline shall interface with Authoritative Data Source systems using Application Program Interfaces (APIs) and standards-compliant open interfaces. The Contractor shall develop any designated system interfaces needed including to/from authoritative data sources as required by their ALD Solution.

5.6.3.1 The Contractor shall provide the design, development, integration, security lockdowns, testing and checkout of the interface to ensure that the transfer requirements and the technical methodology are satisfied.

5.6.3.2 The Contractor shall support Technical Interchange Meeting (TIMs) with Government Interface Partners and document in a System Interface Control Document (ICD) the data transfer requirements to include the data format and the technical methodology to be used to perform the transfer between the ALD and each authoritative data sources and/or content repository. (Interface Control Document, DI-SESS-81248B).

5.7 Phase 1 and 2 Authoritative Data Sources:

A list of phase 1 and phase 2 data sources can be found in file name App_003. Data formats will vary from system to system and can include, but is not restricted to CSV, dat, txt, xml and jpeg.

5.1 Reporting Requirements:

Table 1 - Contract Deliverable List

Data Item Description (DID)	Title	Report Due After Award			
		Initial Submission	Government Review & Comment	Final	Data Rights
Contractor Format with content from	Data Spillage Incident Report	Within 48 Hours of incident	Within 48 Hours of receipt	As Required	Government Purpose Rights

DoDM 5200.01 Vol 3, Enclosure 6					
DI-SESS-81248B	Interface Control Document (ICD)	Initial Submission within 60 days after award, Subsequent submission within 10 days after interface passes integration test	Within ten (10) days of receipt	Ten (10) days before the Phase Ends	Government Purpose Rights
DI-MISC-80508B	Studies and Analysis Report	Within ninety (90) days after award	Same as above	Same as above	Government Purpose Rights
DI-MGMT-82001	Risk Management Framework (RMF) package	Within ninety (90) days after Phase 2 award	Same as above	Same as above	Government Purpose Rights

6.0 PERIOD OF PERFORMANCE.

The Period of Performance (POP) shall be calculated by calendar days with the start commencing one (1) calendar day after notification of award or notification to proceed as:

- **Phase 1 –** Up to 120 Calendar days from contract award
- **Phase 2 –** Up to 245 Calendar days from contract award

7.0 PLACE OF PERFORMANCE.

Performance will be at the Contractor's facility with solution expert support to the Pentagon, Department of the Army Headquarters. The Contractor shall provide ready and knowledgeable support for on-call responses (within :120 minutes) to one-on-one support to Senior Leader users in the Pentagon Department of Army Headquarters during defined and scheduled User Prototype Assessment periods (5 day sessions every 30 days after award. These assessment periods will be scheduled based on the Leaders availability with at least 2 calendar day notification. These assessments will take place on Government business hours/days (Monday-Friday, 9:00am-5:00pm). To permit ease of access, designated Contractor On-Call Support staff will be provided Common Access Card (CAC) badges with either direct access or escorted access to the Senior Leader office.

In addition, the Contractor shall support meetings as needed with the ALD Government Project Team located at two sites:

- Primary: 9531 Hall Rd, (Building 1456 PEO EIS), Fort Belvoir, VA 22206
- Alternate: 2530 Crystal Drive, Suite 1700B, Arlington, VA 22202

8.0 GOVERNMENT FURNISHED EQUIPMENT (GFE), PROPERTY (GFP), MATERIALS (GFM) and DATA (GFD):

The Government will provide the following equipment and support during the prototype project:

- Hosting environment and secure file transfer protocol (SFTP) server with data from the Authoritative Data Sources.
- The Government will sponsor the Interim and Final Clearances as required.
- The Government will sponsor designated Contractor personnel for Common Access Card (CAC) identifications and SIPR tokens

8.1 **Data Access:** Due no later than 10 days after award date, the Government will secure access and authorizations for the data sources which can be found in file name App_003.

8.2 **Network Access:** The Government will provide access to the network environment, including remote access from the Contractor's secure locations, and any required SIPRNet tokens during the Initial Project Work. The Government will also approve use of a data collection/ingestion agent installed on the Government’s network to coordinate ingestion from upstream data sources, which may hold data source credentials provided by the Government. The ALD Prototype Solution system will be initially hosted on a Government Approved Secure Internet Protocol Router Network (SIPRNet). The aggregated data of this capability will reside on a classified, network and be certified and secured in accordance with Army and DoD policies, procedures and regulations. All persons with access to the full range of data visualization capabilities will have appropriate security clearances and authorities to access Army networks in accordance with existing policies and regulations. During this prototype effort, the Army will maintain responsibility for all Army Authoritative Data Sources and associated hardware infrastructure to support the data sets for ALD.

9.0 AGREEMENTS OFFICER REPRESENTATIVE (AOR):

Ms. Mary Harvey
G-3/5/7 (Acquisition Specialist)
PEO Enterprise Information Systems
9350 Hall Rd, Suite 232A
Fort Belvoir, VA 22060
Email: mary.b.harvey8.civ@mail.mil
Desk: 703-806-0098

APPENDIX A: SUPPORTING DOCUMENTATION

1. Definition of Commercially Available (App_001)

2. Data Usage Agreements (App_002)

3. Phase 1 and 2 Authoritative Data Sources (App_003)

4. ALD OV-1 (App_004)