

2. CONTRACT NO. **HE125421C9002** 3. AWARD/EFFECTIVE DATE **30-Aug-2021** 4. ORDER NUMBER

5. SOLICITATION NUMBER 6. SOLICITATION ISSUED DATE

7. FOR SOLICITATION INFORMATION CALL: a. NAME b. TELEPHONE NUMBER (No Collect Calls) 8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE **HE1254** 10. THIS ACQUISITION IS UNRESTRICTED OR SET ASIDE: 100 % FOR:

DOD EDUCATION ACTIVITY
 ATTN: PROCUREMENT DIVISION
 4800 MARK CENTER DRIVE
 SUITE 05F09-02
 ALEXANDRIA VA 22350-1400

TEL:
 FAX:

SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS (WOSB)
 ELIGIBLE UNDER THE WOMEN-OWNED
 SMALL BUSINESS PROGRAM

HUBZONE SMALL BUSINESS EDWOSB NAICS: **541511**

SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS 8(A) SIZE STANDARD: **\$30,000,000**

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
 SEE SCHEDULE

12. DISCOUNT TERMS
Net 30 Days

13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION RFQ IFB RFP

15. DELIVER TO CODE **HF1026** 16. ADMINISTERED BY CODE

DOD INSPECTOR GENERAL (DOD IG)
(b)(6)
 4800 MARK CENTER DRIVE
 ALEXANDRIA VA 22350

SEE ITEM 9

17a. CONTRACTOR/OFFEROR CODE **512C0** FACILITY CODE 18a. PAYMENT WILL BE MADE BY CODE **HQ0791**

KNOWESIS, INC.
(b)(6)
 1115 S. ALAMO STREET, SUITE 2208
 SAN ANTONIO TX 78210-1773

TELEPHONE NO. **(b)(6)**

DFAS-INDIANAPOLIS (DAI DODOIG)
 ACCOUNTS PAYABLE OPERATIONS
 8899 EAST 56TH STREET
 INDIANAPOLIS IN 46249-4500

17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
SEE SCHEDULE					

25. ACCOUNTING AND APPROPRIATION DATA 26. TOTAL AWARD AMOUNT (For Govt. Use Only)

See Schedule **\$1,069,268.80**

27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3, 52.212-5 ARE ATTACHED. ADDENDA ARE ARE NOT ATTACH

27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4, FAR 52.212-5 IS ATTACHED. ADDENDA ARE ARE NOT ATTACH

28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

REF: QTE Received on 13 Aug ust 2021

29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE

30a. SIGNATURE OF OFFEROR/CONTRACTOR 31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

(b)(6)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT) 30c. DATE SIGNED 31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) 31c. DATE SIGNED

(TYPE OR PRINT)

GEORGETTE HENDRICKSEN / CONTRACTING OFFICER 27-Aug-2021

TEL: **(b)(6)**

EMAIL: **(b)(6)**

Inspect By DoDAAC	HE1026
Ship To Code	HE1026
Service Approver (DoDAAC)	HE1026
Service Acceptor (DoDAAC)	HE1026

(4) Payment request. The Contractor shall ensure a payment request includes documentation appropriate to the type of payment request in accordance with the payment clause, contract financing clause, or Federal Acquisition Regulation 52.216-7, Allowable Cost and Payment, as applicable.

(5) Receiving report. The Contractor shall ensure a receiving report meets the requirements of DFARS Appendix F.

(g) WAWF point of contact.

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

(b)(6)

(2) Contact the WAWF helpdesk at 866-618-5988, if assistance is needed.

(End of clause)

PERFORMANCE WORK STATEMENT

PERFORMANCE WORK STATEMENT FOR Cloudera Installation and Configuration

1. General Information and Scope of Work.

1.1 Agency: The Department of Defense Office of the Inspector General (DoD OIG) serves under the provisions of Public Law 95-452 as an independent and objective official responsible for conducting, supervising, monitoring and initiating audits, investigations and inspections relating to DoD programs and operations.

1.2 Background: The goal of the Data Analytics Program (DAP) is to increase the OIG's ability to identify and focus oversight resources on high risk areas, i.e., health and safety concerns, fraud, waste, and abuse of DoD resources. This is accomplished through the use of computer-based analytical techniques that rely upon current software technology, availability of DoD source data, and subject matter experts (SME) to make recommendations that fix internal control problems, reduce or eliminate waste and inefficiencies, and arrest and refer those who engage in criminal activity for prosecution. Our immediate need is to support on-going projects and expand data analysis capabilities in order to accomplish a variety of data analytics functions with a scalable file system and analysis tool set.

1.3 Scope of work: The contractor shall provide all personnel, equipment, supplies and materials, transportation, tools, supervision, and other items and non-personal services necessary to provide integrated and optimized software for the existing OIG environment, as well as, services to ensure the software is properly supported throughout the period of performance as discussed in this Performance Work Statement (PWS).

2. Requirement (Objectives).

The objective of this PWS is to obtain Commercial off-the-shelf (COTS) software subscriptions and contractor support to install, configure, maintain, and upgrade COTS software at a Government facility in the Continental United States (CONUS) on both NIPR and SIPR environments. The DOD OIG requires an accessible Agency-wide analytics platform that provides an integrated environment for predictive and descriptive modeling, data mining, text analytics, forecasting, optimization, simulation, and experimental design. The contractor shall provide the software, licensing, technical support, and maintenance for each instance of software and its components. The contractor shall be responsible for on-site service, as required, to support the successful completion of all tasks and objectives of the PWS.

2.1 Software Acquisition (Objective 1).

The contractor shall provide COTS software subscription solutions in accordance with the requirements within this PWS. The contractor shall be responsible for on-site service, as required, to support the successful completion of all tasks and objectives of the PWS and additional customer support that may be required for each instance of software and components licensed and installed.

2.1.1 (Task 1) The following software subscriptions, including maintenance, will be required. For additional specifications, please see Section 8.

- Cloudera Data Platform, Version 7 (or newer);
- Cloudera Data Science Workbench;
- Cloudera Data Flow (includes Apache NiFi; Apache Kafka, etc);
- JIRA (Data Center);
- ArcGIS Enterprise;

Performance Standards and Acceptable Quality Levels

The following applies to Objective 1:

2.1.2 Performance Standard (PS1) – Task shall be completed no later than 23 August 2021 and in accordance with the PWS; then annually with each exercised option.

2.1.3 Acceptable Quality Level (AQL 1) – No Deviation from the Performance Standard.

2.2 Services to Install, Migrate, and Maintain Software (Objective 2).

The Contractor shall complete installation, configuration, testing, project migration, and knowledge transfer, as required in Section 2.2.3, to ensure software is installed and maintained within the DoD OIG environment.

2.2.1 Project Management (Task 1)

2.2.1.1 The contractor shall maintain a Risk Register. The Risk Register will include all identified risks associated with the installation, configuration, optimization and validation of specified software. A risk is any issue identified by the contractor or the OIG which may delay or prevent the success of the installation, configuration, optimization and validation of specified software. All entries on the risk register will include at a minimum a definition of the risk, a priority rating (based on potential impact and timeline to mitigate or minimize the impact), the date the risk was identified, and the person who identified the risk. The OIG shall provide a format for the risk register shortly after contract award. **Deliverable: Risk Register**

2.2.1.2 The contractor shall coordinate with OIG to develop and maintain a Project Plan which outlines all tasks and milestones, including associated timelines and responsible personnel, (OIG staff and, or Contractor staff as applicable) which are required to successfully install, configure, optimize and validate specified software. Updates to the Project Plan which affect timelines for major milestones will be briefed to the COR as soon as the need for revision is identified. **Deliverable: Project Plan**

2.2.1.3 The Contractor shall conduct an initial Kick-Off Meeting and then regular status briefings to address: work performed, upcoming work, any issues, unresolved risks and any other information which is current and relevant to the performance of the work outlined in this performance work statement. The status briefings and meetings: agendas, minutes, action items and sequence plans as applicable. The schedule of delivery of these briefings may be adjusted as the COR deems is necessary; under normal circumstances OIG anticipates that in-person bi-weekly progress meetings, weekly touch point telephone conversations, and monthly in person executive briefings will be sufficient. Exceptions shall be made requiring additional briefings as necessary in the event of critical issues which may affect the project schedule. The Kick-Off Meeting shall address the following:

- Understand use case and success criteria
- Finalize cluster, security requirements including Kerberos and AD integration
- Develop Cluster and Components Design
- Security solution design
- Documentation and Knowledge Transfer
- Complete current state discovery questionnaire
- Complete Upgrade risk assessment questionnaire
- Finalize Hive upgrade path
- Pig/flume migration plan, if relevant
- Validate OS upgrade and other pre-requisites
- Understand F5 role and support
- Software testing and acceptance criteria

Deliverable: Initial Kick-Off Meeting and Regular Status Briefings
Deliverable: Technical Documentation or Manuals Outlining Typical Installation, Configuration, and Migration Steps

2.2.2 Pre-Installation Walkthrough and Planning (Task 2)

- 2.2.2.1 The Contractor shall host planning meeting(s) to create a comprehensive Engineering Plan that includes all software in this PWS. The Engineering Plan will include technical descriptions of required resources, services which the Big Data Platform software systems are dependent on, network communication ports, and include any other information which Office of the Chief Information Officer (OCIO) may require. The Engineering Plan shall ensure that the system will utilize CAC authentication for users wherever user authentication is required. User authentication shall be required in order to access any data set in any manner. That is, users must authenticate before interacting with data in order to ensure that the appropriate level of access is possessed by a user for any data. The engineering plan shall be constructed to ensure that system users will be able to perform any advertised capability of the specified software. The Engineering plan includes a System Architecture Design. This document shall be approved by Office of the Chief Information Officer (OCIO) personnel through the COR prior to implementing any changes to Information Systems. Any necessary modifications to the Engineering Plan shall also be approved by appropriate OCIO Personnel. The contractor shall be provided by the OIG, an example of this document upon contract award. **Deliverable: Engineering Plan**
- 2.2.2.2 The Contractor shall consult with OIG as necessary, to develop a System Architecture Design. The System Architecture Design will ensure that the specified software, software subcomponents and hardware are appropriately configured to support the OIG's current and desired analytic capabilities. The System Architecture will include the arrangement and relationships between all system components, for example servers, clients and other dependent and supporting information systems **Deliverable: System Architecture Design**
- 2.2.2.3 The Contractor shall develop a detailed Installation and Configuration Procedure which will outline all required steps to install and configure all specified Big Data Platform software. The Procedure will include screen capture images and instructions for each step required to install and configure all of the specified Big Data Platform software. **Deliverable: Installation and Configuration Procedure**
- If, during the course of the installation and configuration, it becomes necessary to deviate from this procedure, the procedure will be modified to reflect those necessary modifications.
- 2.2.2.4 The Contractor shall assist the OIG as necessary to ensure that the required computing resources are available and properly configured in order to ensure the successful installation, configuration, optimization and validation of the specified software. For resources which are specifically under the control of the OIG, the contractor will work with OIG to schedule the performance of necessary tasks.
- 2.2.3 Software, Installation and Configuration (Task 3)**
- 2.2.3.1 The Contractor shall work with OIG personnel to install, configure, and optimize all Cloudera software, verify that JIRA and ArcGIS have been installed and configured into the OIG's computing environments. The contractor shall ensure that the installation and configuration is performed in accordance with the Installation and Configuration Procedure and the Engineering Plan.

Deliverable: Record of Installation tasks

- 2.2.3.2 The Contractor shall ensure the correct performance of all tasks necessary to install and configure the specified software in order to enable a user of any of the specified software to perform all advertised capabilities of that software. Demonstration of encryption of all software communication.
- 2.2.3.3 For all environments, the Contractor shall transfer to OIG personnel all knowledge which is required to repeat all necessary installation and configuration steps. This includes: basic training material such as manuals, walkthroughs, and web-based material (as long as the material can be accessed from our network). **Deliverable: Technical Documentation as required for Knowledge Transfer**
- 2.2.4 Software Testing (Task 4)**
- 2.2.4.1 The software installation in each environment shall be verified through functional testing as agreed to Task 2 (section 2.2.2) and shall demonstrate all software is capable of performing advertised capabilities and adheres to all DOD and OCIO guidance. In addition, the Contractor should consider the following when developing a test plan:
- Any installation or configuration errors identified during the execution of a testing plan will be remediated. Demonstration of encryption of all Big Data Platform Software communications:
 - Leverages Secure Sockets Layer (SSL) to facilitate secure HTTPS communication between all web clients and the cluster.
 - A layer of encryption when data is in transit between nodes.
 - A layer of encryption when data is in transit between the cluster and thick clients.
 - Demonstration of authorization, authentication and access amongst the application, the user's Common Access Cards (CAC), and active directory. *The expectation is that the suite of Cloudera applications will leverage the user's CAC and OIG's active directory to verify the user is authorized to access Cloudera applications, authenticates the user's CAC to the active directory, and either allows that authorization to persist while accessing each Cloudera application (managed centrally) or challenges and authenticates at each entry point.*
 - Secure login using CAC credentials to the application's web clients, to include the prevention of non-authorized user accounts from logging into web clients.
 - Secure login using CAC credentials to the application's thick clients
 - Secure login for Administrative Accounts to the application's software; prevention of non-authorized user accounts from logging into the application and Administration functions.
 - Any specified tests to demonstrate compliance with all DOD, OCIO, or standard operating procedures at the OIG in order to obtain certification for production status.
 - Demonstration of data provenance/data lineage tracking.
 - Demonstration of secure and governed data ingestion, data transformation and content routing.

- Demonstration of key features of the CDP such as management console, workload manager, data catalog, replication manager, data hub, data warehouse, machine learning, and Cloudera runtime.

- 2.2.4.2 The Contractor, for each environment, shall develop a Testing Plan. The Testing Plan is a list of steps to be performed which will confirm that all specified software has been installed and configured as required in order to enable a user of the specified software in the OIG computing environment to perform all of the advertised capabilities of the specified software. The COR shall approve the Installation Testing Plan prior to the performance of Installation Testing. It is not necessary that the Installation Testing Plan test all advertised capabilities, only that the tests, when successfully performed are sufficient to ensure that the advertised capabilities of the specified software can be performed. **Deliverable: Testing Plan(s)**
- 2.2.4.3 The Contractor shall assist OIG personnel in completing all steps of the Installation Testing Plan under the supervision of the designated Subject Matter Expert and the COR for each environment. **Deliverable: Performance of test plan(s)**
- 2.2.4.4 The results of the Testing shall be recorded by the contractor for each environment. **Deliverable: Record of Test Results by Environment**
- 2.2.4.5 In the event that any of the tests fail, the Contractor shall develop a Technical Remediation Plan which includes a technical explanation of why the test failed and the steps necessary to correct the installation and configuration in order to facilitate a successful test. The Contractor shall update, as applicable any parts of the Installation and Configuration Plan and the Engineering Plan. **Deliverable: Technical Remediation Plan (if necessary)**
- 2.2.4.6 The Contractor shall record all remedial actions which are necessary to facilitate successful performance of the Testing Plan. **Deliverable: Record of Remedial Action (if necessary)**
- 2.2.5 Migration (NIPR Environment Only) (Task 6)**
- 2.2.5.1 The Contractor shall work with OIG personnel to migrate all existing projects at the start of the engagement to the new environment. This shall include a written plan with steps to migrate. **Deliverable: Migration Plan**
- 2.2.5.2 The Contractor shall demonstrate that projects were successfully migrated into the new environment and update the Migration Plan to reflect actual steps taken to migrate and test. **Deliverable: Update Migration Plan**
- 2.2.6 Resident Solutions Architect Services (Task 7)**
- 2.2.6.1 The Contractor shall provide regular, routine support throughout the performance period to assist with, but not limited to, the following: installation and configuration is at optimal specifications, environments are fine-tuned to avoid issues, assist with preparing for planned projects, assist with automating entire project lifecycle, assist

with incremental updates and upgrades; assist with migrating critical projects, assist with implementing security; and assist/demonstrate advance administrative duties. In addition, shall assist with new use cases (i.e., analytics/ML, data science, data ingest and processing) Infrastructure (including new cluster deployments, cluster migration, expansion, major upgrades, COOP/DR, and security)

- 2.2.6.2 Resident Solutions Architect (RSA) or similar, along with a Senior Service Delivery Manager, shall provide a variety of services, as outlined in Section 2.2.6.1, throughout the POP on a monthly basis as agreed-to during monthly status meetings with the Senior Service Delivery Manager or equivalent.

Deliverable: Planned Tasks, Schedule, and Outcome

2.2.7 Maintenance (Task 8)

- 2.2.7.1 The contractor shall provide standard maintenance during the performance of the contract for all of the specified software including at a minimum: providing standard technical support for system users, data managers, and system administrators; providing updates to any specified software or required software subcomponent.

Deliverable: Cloudera Ticket and Resolution

Performance Standards and Acceptable Quality Levels (Objective 2)

The following applies to Objective 2:

- 2.1 Performance Standard (PS1) - Tasks will be completed by the required completion date

Acceptable Quality Level (AQL 1) - 95 % of tasks will be completed by the required completion date. The remaining 5% shall be completed no later than 10 days after their due date.

2.3 Travel (Objective 3).

Travel is expected for Software Installation (Objective 2) on an as needed basis. Travel will consist of one CLIN with two SCLINS.

SCLIN 1 (Airfare/Car Rental)

The first SCLIN for travel shall be for airfare and car rental. The contractor will be asked to provide the airfare price for each travel event. The Government will then use independent market research to determine the reasonableness of the price. The Government will only reimburse the contractor for the agreed upon airfare determined prior to travel. Airfare shall only be purchased at economy/coach class levels unless the contractor can present evidence, which the Government can confirm, on the unavailability of economy/coach class seating options for a specific trip. Car rental: no car larger than an economy size should be rented. Rental above economy size shall be justified prior to travel. Claims for rental car gasoline shall be supported by original receipts.

SCLIN 2 (Per Diem)

The second SCLIN shall be for Per Diem which shall be calculated using GSA's annual rates at time of travel found at <https://www.gsa.gov/perdiem>. For example, a trip to Los Angeles, CA has a 2019 Per Diem rate of \$180 for the month of June. Any Government approved travel occurring during the

month of June in 2019 shall have a fixed Per Diem rate of \$180 per GSA's established rates at time of travel.

No other expenses outside of Airfare and Per Diem shall be reimbursed resulting from travel associated with the contract.

Task 1 – Travel Plans: The contractor shall provide a detailed travel plan in support of the objective(s) to the COR no less than ten (10) business days prior to travel unless the travel is in response to an emergency as determined by the Government. The travel plan shall include the name of the traveler(s), location, purpose, and dates of travel; and a breakdown of anticipated travel expenses (rental car, airfare, etc.). The Contractor shall coordinate with the OCIO to ensure site notification no less than ten (10) business days prior to the requested travel date.

Performance Standards and Acceptable Quality Levels (Objective 3)

The following applies to Objective 3:

PS1 –Complete tasks within agreed upon timelines.

AQL1 – No deviation.

3. Constraints.

3.1 Period of Performance: The period of performance of the base year shall be 12 months upon award. The Government and Contractor may mutually-agree to exercise the option to extend the terms of the contract for an additional annual term(s). The period of performance shall be one (1) base year upon award, plus up to two (2) option years if exercised by the Government.

3.2 Security requirements

3.2.1 Security Clearance requirement

3.2.1.1 This contract is a SECRET, and the Contractor must have a FINAL SECRET CLEARANCE. The Contractor shall provide proof that personnel who will be performing work on site under this contract possess, at a minimum, a SECRET clearance at the time of award of the contract and shall maintain this minimum level of security for the duration of the contract. It is the contractor's responsibility to ensure that all security requirements are followed in accordance with 5200.2 DoDM 2017, Procedures of the Personnel Security Program.

3.2.1.2 The contractor shall implement security requirements as defined below and approved by the OIG.

All contractor personnel background investigations will be verified by OSEC prior to performance. For personnel needing sustained access to the facilities or access to OIG Information Systems (IS) in order to perform on the contract, the contractor shall submit a visit authorization letter (VAL) via the Joint Personnel Adjudication System (JPAS) or Defense Information System for Security (DISS) to the Industrial Security Program Manager (ISPM) in the Office of Security (OSEC). The VAL shall be submitted a minimum of fourteen (14) days prior to the anticipated date on which facilities or IS access is required.

- 3.2.1.3 The contractor shall ensure that all contractor personnel working on this project who will have visibility of Personally Identifiable Information (PII), Privacy Act information, and other types of Unclassified Sensitive Information, comply with the DoD Privacy Program and the Non-Disclosure Agreement. The DoD Privacy Program (32 CFR 310, Part 310/DoDD 5400.11) provision restricts contractor employees from disclosing PII from a system of records they operate on behalf of a DoD component, outside of DoD. All contractor personnel assigned tasks which require access to information from Secret to Personally Identifiable Information (PII), Privacy Act information, and other types of Unclassified Sensitive Information must complete and submit a Classified Non-Disclosure Agreement (SF 312) to the OIG Office of Security (OSEC) prior to acquiring accessing such data. A copy of the applicable Classified Non-Disclosure Agreement (SF 312) will be provided to the Contractor by the COR as needed. During the performance of the work of this PWS, various datasets to be worked with will be identified by the Government. The particular NDA, which would be required for a given dataset, will vary depending on which data is selected by the government.
- 3.2.1.4 The Contractor is responsible for ensuring that all persons working on the program are U. S. citizens. Therefore, Contractor personnel who currently hold dual citizenships and/or active foreign passports must report possession of a foreign passport to their Company Facility Security Officer (FSO). Contractor personnel must report any use of a foreign passport to enter or exit the United States to the FSO. The FSO shall follow guidelines as set forth within the SECURITY EXECUTIVE AGENT DIRECTIVE 4 (SEAD 4). There is no guarantee that the individual will be permitted to perform on this program.
- 3.2.1.5 The Government reserves the right to have any contractor employee removed, whenever there is probable cause to believe, on the basis of all facts available, that such action is warranted in the interest of national security. This action shall be made whether or not the cause is deemed of sufficient severity to warrant action to terminate the contractor's Facility Clearance or individual security clearance. The Government also reserves the right to remove any contractor on the basis of alleged misconduct which may, in the opinion of the Contracting Officer, jeopardize the security of the project.

3.2.2 Building access

- 3.2.2.1 The primary place of performance, Mark Center, Alexandria VA, is a controlled facility and requires all visitors to request access.
- 3.2.2.2 A CAC will be required for access to the facilities and access to OIG Information Systems. All CACs issued to contractor personnel are government property and must be returned either upon departure from the program or at the conclusion of the contract (whichever comes first) to the Industrial Security Program Manager.

DoD, Office of Inspector General
Office of Security
Attn: Industrial Security Program Manager
4800 Mark Center Drive, Room 9B24
Alexandria, VA 22350-1500

- a) Network Access: Before access to the DoD OIG network is granted to contractor personnel, the following information shall be provided to the COR. User Agreement: A signed copy of the DoD OIG User Agreement and provide the agreements to the COR no later than 20 days after being approved to work on the contract.

All contractors are required to complete the annual mandatory training listed below. All Certificates of Completions are to be turned into the COR no later than 20 days after being approved to work on the contract:

- i. Cyber Awareness Challenge.
- ii. Anti-terrorism Training Level 1:
- iii. Personally Identifiable Information (PII) training,
 1. The contractor is required to safeguard PII in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and DoD privacy policy in effect during the period of performance. The DoD OIG must be informed within 24 hours if DoD PII data is compromised, lost, or stolen. Depending on the nature of information compromised, lost, or stolen, the Government has the right to invoke appropriate disciplinary action which may include civil and criminal penalties as outlined in DoD Regulation 5400.11-R, May 14, 2007.
- iv. Preventing Work Place Violence
- v. DoD OIG Initial Security Training.
- vi. DoD OIG Annual Security Awareness Refresher.
- vii. Counterintelligence Awareness and Reporting Training.
- viii. Insider Threat Awareness.
- ix. Operations Security (OPSEC) TRAINING.
- x. Unauthorized Disclosure of Classified Information for DoD and Industry.
- xi. Introduction to Information Security.

Special Qualifications: N/A

3.3 Hours of Operation: The Contractor is responsible for providing services, between the hours of 7:00 am and 6:00 pm (EDT and CDT) Monday through Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, designated by Federal Statute, Executive Order, or Presidential Proclamation. The ten Federal holidays include New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving, and Christmas Day. OIG shall provide for the Contractor a means of determining whether or not the facilities are open.

3.4 Place of Performance: The work to be performed under this contract will be primarily performed at 4800 Mark Center Drive, Alexandria, VA 22311. Additional, but limited work, may be required at 401 E. Moore Drive MAFB, Gunter Annex, AL 36114. Remote work for ongoing maintenance and trouble-shooting is permissible using OCIO-approved teleworking and communication methods. All work in the SIPR environment shall be performed within Government facilities with no exceptions.

3.5 Key Personnel: The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to diverting any of the specified individuals to other programs or contracts (or as soon as possible, if an individual must be replaced, for example, as a result of leaving the employ of the Contractor), the Contractor shall notify the Contracting Officer and shall submit comprehensive justification for the diversion or replacement request (including proposed substitutions for key personnel) to permit evaluation by the Government of the impact on performance under this contract. The Contractor shall not divert or otherwise replace any key personnel without the written consent of the Contracting Officer. The Government may modify the contract to add or delete key personnel at the request of the contractor or Government.

The Contractor shall provide a Contract Manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the Contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available during the hours listed in section 3.3 of the PWS.

All contract personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed.

4. Government-Furnished Resources.

4.1.1 Personnel: The Contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

4.1.2 Facilities: The Government will furnish the necessary workspace for the contractor personnel to provide services outlined in this PWS as required.

4.1.3 Utilities: All utilities in the facility will be available for the contractor's use in performance of duties outlined in this PWS. The Contractor shall instruct contractor personnel in utilities conservation practices. The Contractor shall be responsible for operating under conditions that preclude the waste of utilities.

4.1.4 Equipment: The Government will provide appropriate access to IT resources such as servers and workstations, and typical office equipment such as printers, copiers, etc. as

required by the Government in order to ensure the timely and efficient completion of the Contractors work.

- OCIO standard issue laptop and monitor.
- SIPRnet Token and elevated rights, if deemed necessary by OCIO
- Elevated/Administrative Rights needed to complete the installation of all software, subject to OCIO approval (each Contractor requesting elevated rights must show proof of completing security+ certification or equivalent per OCIO guidance)
- Connection to DoD OIG SIPR Network through assigned DoD OIG system administrator to facilitate the installation/configuration.
- An assigned DoD OIG system administrator to facilitate requests for all required Public Key Infrastructure (PKI) and Certificate Authorities.

4.1.5 Materials: The Government will provide standard operating procedures and policies, network topology diagrams, and standard forms.

In performance of this contract, the Contractor shall furnish all supplies, equipment, facilities and services required that were not already provided by the Government to perform work under this contract and are not listed under Section 3 of this PWS.

5. Contract Deliverables.

Technical Exhibit 1 – Summary Schedule of Deliverables:

This table contains a summary of deliverables contained within this PWS. Full definitions of deliverables are contained in the information above.

<u>MILESTONE/ DELIVERABLE</u>	<u>FORMAT</u>	<u>NUMBER Copies</u>	<u>PWS Reference</u>	<u>PLANNED Frequency</u>
Technical Documentation or Manuals Outlining Typical Installation, Configuration, and Migration Steps (Digital Documents of manuals or walkthroughs, and Web-based material)	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	3 copies: 1 to COR, 2 to TPOCs (designated at Kickoff)	Section 2.2.1	30 days after contract award
Risk Register	Excel Spreadsheet	N/A	Section 2.2.1	Initial 45 days after contract award; then updates every 30 days thereafter
Project Plan	Microsoft © Project digital document (.mpp file)	3 copies: 1 to COR, 2 to TPOCs (designated at Kickoff)	Section 2.2.1	Initial 45 days after contract award; then updates every 30 days thereafter
Kick Off & Regular Status Briefings	Telephone conference calls & in-person meetings (as defined above, or agreed upon by the Contractor and the COR)	N/A	Section 2.2.1	Kick Off within 10 days after contract award; Status Briefings – initial 5 days after Kick Off then updates every 30 days thereafter

Engineering Plan	Digital Document (format provided at kick-off)	2 copies to the COR	Section 2.2.2	45 days after contract award or As agreed-to at kick-off meeting
System Architecture Design	Digital Document (format provided at kick-off)	2 copies to the COR	Section 2.2.2	45 days after kick-off or As agreed-to at kick-off meeting
Installation and Configuration Procedure	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.2	45 days after kick-off or As agreed-to at kick-off meeting
Executable installation files/ Licenses delivered in OEM specified format	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	1 copy to the COR and 1 copy to the TPOC designated at Kickoff	Section 2.1	10 days after contract award
Record of Installation	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.3	100 days after contract award or As agreed-to at kick-off meeting
Technical Documentation as required for Knowledge Transfer	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.3	100 days after contract award or As agreed-to at kick-off meeting
Testing Plan	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.4	110 days after contract award or As agreed-to in the project plan
Performance of Test Plan	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.4	120 days after contract award or As agreed-to in the project plan
Record of Test Results by Environment	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.4	125 days after contract award or As agreed-to in project plan/testing plan
Technical Remediation Plan (if necessary)	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.4	130 days after contract award or As agreed-to in project plan/testing plan; then updates every week thereafter
Record of Remedial Action (if necessary)	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.4	2 days after each remediation action or As agreed-to in the project plan
Migration Plan	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.5	135 days after contract award or As agreed-to in project plan/testing plan
Updated Migration Plan	ELECTRONIC (e.g. MICROSOFT WORD OR .PDF)	2 copies to the COR	Section 2.2.5	145 days after contract award or As agreed-to in

				project plan/testing plan
Planned Tasks, Schedule, and Documentation of Tasks	Email	1 copy to COR and 1 copy to TPOC	Section 2.2.6	Tasks/Schedule 5 days prior to engagement; Documentation of Tasks 5 days after engagement
Maintenance Summary		1 copy to COR and 1 copy to TPOC	Section 2.2.7	Copy of maintenance action/requests as they occur and confirmation and outcome when closed

6. Acronyms and Definitions. Alphabetical list of definitions of key words used or acronyms.

Definitions:

ADVERTISED CAPABILITY. The term “advertised capability” is defined as any feature or function which Big Data Platform SOFTWARE claims that the specified software is capable of performing. These claims may be written in Big Data Platform SOFTWARE advertisements. These claims are specific and unique to particular versions of the specified software. **CONTRACTOR.** A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

CONTRACTING OFFICER (KO). A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

DELIVERABLE. Anything that can be physically delivered, but may include non-manufactured/physical things such as meeting minutes or reports.

IDEAL PERFORMANCE LEVELS. The response time of a software system as defined by benchmark testing for a given amount of resources under optimal circumstances.

KEY PERSONNEL. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

QUALITY ASSURANCE. The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards. (Or those actions taken by the government to assure services meet the requirements of the Performance Work Statement.)

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

QUALITY CONTROL PROGRAM. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

SERVICE INTERRUPTION. A service interruption is any event which prevents or impairs a user's or administrator's ability to interact with the system.

SPECIFIED SOFTWARE. See the list of specified software in Section: 7.2. This phrase also refers to any required software subcomponents.

SUBCONTRACTOR. One that enters into a contract with a prime Contractor. The Government does not have privity of contract with the subcontractor.

SYSTEM. The collection of licensed Software applications (server or client) and hardware (physical or virtual). **WORK DAY.** The number of hours per day the Contractor provides services in accordance with the contract.

WORK WEEK. Monday through Friday, unless specified otherwise.

Acronyms:

CAC	Common Access Card
CFR	Code of Federal Regulations
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer's Representative
COTS	Commercial-Off-the-Shelf
DFARS	Defense Federal Acquisition Regulation Supplement
DoD/DOD	Department of Defense
DCSA	Defense Counterintelligence and Security Agency
FAR	Federal Acquisition Regulation
GFE	Government Furnished Equipment
GFP	Government Furnished Property
HIPAA	Health Insurance Portability and Accountability Act of 1996
OCIO	Office of the Chief Information Officer
ISPM	Industrial Security Program Manager
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulation
KO	Contracting Officer
OIG	Office of the Inspector General
OPSEC	Operation Security
OSEC	Office of Security Service

POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
TE	Technical Exhibit
VAL	Visit Authorization Letter
VCC	Visitor Control Center

7. Performance Requirement Summary (PRS).

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Technical Exhibit 2 - Performance Requirements Summary

Performance Objective	Performance Standard	Performance Threshold/AQL	Method of Surveillance
Objective 1 (Software Acquisition) PWS Para 2.1 Task 1	Tasks shall be completed no later than 31 December 2021 and in accordance with the PWS	No deviation	Periodic Surveillance through observation, Status Meetings and Reports.
Project Management (Section 2.2.1)	Deliver Risk Register, Project Plan, Regular Status Briefings, Agendas minutes and action items	Acceptable Quality Level = 95%	INSPECTION
Pre-Installation Walkthrough and Planning (Section 2.2.2)	Deliver: Documented meeting notes, Engineering Plan, System Architecture Design, Installation and Configuration Procedure	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION
Installation and Configuration (Section 2.2.3)	Deliver: A fully installed and configured Big Data Platform SOFTWARE as designed in the Engineering Plan, Updated Installation and Configuration Procedure, Updated Engineering Plan, Updated Technical Documentation as required for Knowledge Transfer, Record of Installation tasks	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION
Testing (Section 2.2.4)	Deliver: Testing Plan, Performance of test plan, Record of Test Results, Technical Remediation Plan (if necessary), and Record of Remedial Action (if necessary). Deliver at a minimum, a project plan, detailed documented processes by which work	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION

	was performed in order to accomplish the objectives.		
Migration (Section 2.2.5):	Deliver: Migration Plan and Updated Migration Plan that includes detailed documented processes by which work was performed in order to accomplish the objectives.	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION
Resident Solutions Architect (Section 2.2.6):	Deliver: Planned Tasks, Schedule, and Documentation of Tasks. The contractor shall provide Cloudera RSA services during the POP for all of the specified software that includes summary of documented processes by which work was performed in order to accomplish the objectives.	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION
Maintenance (Section 2.2.5):	The contractor shall provide standard maintenance during the POP for all of the specified software including at a minimum: providing unlimited technical support for system users, data managers, and system administrators; providing updates to any specified software or required software subcomponent.	Acceptable Quality Level = 95%	PERIODIC SAMPLING and PERIODIC INSPECTION

7.1 Quality Control Plan

Quality Control Plan: The Contractor shall develop and maintain an effective Quality Control Plan (QCP) to ensure that services are performed in accordance with the PWS. The Contractor's QCP is the means by which the Contractor assures that the work complies with the requirement of the contract. The QCP is to be delivered within 30 days after contract award. The quality control program shall be delivered to the Contracting Officer Representative (COR) within 30 calendar days of the DOA. The COR shall review and approve the quality control program within 15 calendar days after submission by the contractor, or provide comments showing additional information required. The contractor shall then address all COR comments and provide additional requested information to the COR within 15 calendar days from receipt. The review and correction timeframe for the deliverable shall not exceed 30 calendar days from the date of the initial receipt by the COR. After acceptance of the quality control plan, the contractor shall receive the COR's acceptance in writing of any proposed change to his quality control system.

7.2 Quality Assurance Surveillance Plan (QASP)

The Government will utilize a QASP to monitor the contractor's performance on the contract. The QASP is a living document and can change at any time during the life of the contract. As such, the Government reserves the right to unilaterally edit the QASP at the Government's discretion.

8. Software Specifications.

The software shall meet all of the specifications listed below:

Salient Characteristics

- Software that can simultaneously distribute data, queries, statistical, and other advanced procedures across multiple servers (nodes) for processing.
- Should allow agile application deployment, new machine learning/deep learning workloads, real-time data warehousing, & security and governance.
- Must allow multiple instances of the application to run to be able to develop and test new versions of services without the older versions being disrupted.
- Ability develop and prototype new machine learning projects and easily deploy them to production.
- Single Sign On (SSO) using two-factor authentication using smart cards (known within DoD as the Common Access Card or CAC).
- Include Apache Spark and/or a Data Science Workbench (or similar) that can deploy advanced statistical and Natural Language Processing (NLP) across the file system.
- Software solution must operate with a high degree of fault tolerance and incrementally scale processing capability with additional nodes to add to the overall capacity of the entire system.
- Software deployment onsite at OIG Headquarters (Mark Center, Alexandria, VA) and within a DISA-hosted Data Center to align with our IT department's strategic plan.
 - Contractor shall provide the following software subscriptions:
 - **NIPR Environment**
 - Cloudera Private Cloud Base – USCSS – US Based Support 20 nodes
 - Production: 16 physical nodes
 - Staging: 4 virtual nodes
 - Total compute variable 480 (COMPUTE: price per CCU per year for compute in excess of 16 cores/128GB RAM per Node, where 1CCU = 1 core + 8 GB RAM)
 - Cloudera Data Science Workbench (CDSW)
 - NIPR: 20 named users base, add 5 named users each option year
 - Cloudera DataFlow (CDF)
 - NIPR: See Production specifications above. Installation on nodes/cores as required to be fully functional.
 - Includes full advertised stack to include, but not limited to, the following: Edge and Flow Management (Apache NiFi, MiNiFi, Edge Flow Manager); Stream Processing and Analytics (Apache Flink, SQL Stream Builder, Kafka Streams); Streams Messaging (Apache Kafka, Streams Messaging Manager, Streams Replication Manager)
 - **SIPR Environment**
 - Cloudera Private Cloud Base – USCSS – US Based Support 16 nodes
 - Production: 16 physical nodes

- Total compute variable 480 (COMPUTE: price per CCU per year for compute in excess of 16 cores/128GB RAM per Node, where 1CCU = 1 core + 8 GB RAM)
- Cloudera Data Science Workbench (CDSW)
 - SIPR: 10 named users base, add 5 named users every other option year

Professional Services

- Option Year 1-4: 480 hours of Cloudera Resident Solutions Architect (RSA) with Senior Service Delivery Manager

Point of Contact: HE125421C9002

Contracting Officer

Name: Kellie Buck

Email: (b)(6)

Contract Specialist

Name: Michele Maxwell

Email: (b)(6)

Program Manager

Name: (b)(6)

Email: (b)(6)

COR

Name: (b)(6)

Email: (b)(6)