Performance Work Statement
for
Development Security Operations, Hosting, and Software Support

1. Background

The Army Analytics Group (AAG) provides system configuration and analytical services for the Army's senior leadership and innovative application and data integration services across the Enterprise. AAG provides problem solving capabilities that involve massive enterprise data integration and analysis is coupled with the most advanced Information Technology (IT) solutions.

Additionally, AAG provides software maintenance and enhancements for AAG managed/supported applications; Data Integration and Transformation services for AAG supported applications; Provides Security Code Scanning and documentation for AAG managed applications; Provides quality assurance supporting data integration and transformation services for AAG managed applications; Provides Configuration and Change management services for AAG managed applications.

Army Directive 2024-02 (Enabling Modern Software Development and Acquisition Practices) established policy and assigns responsibilities for the Army's adoption of modern software development and acquisition practices. For the purposes of this policy, modern software development practices include, but are not limited to, continuous integration/continuous delivery (CI/CD), agile, lean, and Development, Security, and Operations (DevSecOps).

An organizational software engineering culture and practice that aims at unifying software development DevSecOps. The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle. In DevSecOps, testing and security is now an automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously (DoDI 5000.87).

1.1 GENERAL INFORMATION:

This is a non-personal service(s) contract under which the personnel rendering the service(s) are not subject, either by the contract’s terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its employees.

1.1.1 Period of Performance

The period of performance consists of five (5) years made up of a one (1) year base period plus four (4) one year option periods. The period of Performance is depicted below:

Base Period:	Date of award through calendar day 365
Option Period One (1):	Calendar day 366 to calendar day 730.
Option Period Two (2):	Calendar day 731 to calendar day 1,095.
Option Period Three (3):	Calendar day 1,096 to calendar day 1,460.
Option Period Four (4):	Calendar day 1,461 to calendar day 1,825.

1.1.2 Place of Performance

The primary work performed under this contract shall be performed at Fairfield, CA.

1.1.3 Telework: Teleworking will only be approved on a case-by-case basis at the Government's convenience on UNCLASSIFIED work only.

1.1.4 Travel: Periodic travel maybe required in order to perform the requirements of this PWS. Travel is defined as any trip outside a 50-mile radius of Fairfield, CA. All travel requests shall be approved by the Contracting Officer Representative (COR) prior to commencement of travel. All requests shall be approved before commencement of the travel and submitted utilizing the AAG approved Travel Request. The contractor shall submit a trip report (CDRL A0012, DI-MISC-81943, Trip/Travel Report) to the Government within 10 days following the conclusion of the travel. The government will reimburse travel in accordance with the Joint Travel Regulations (JTR) and FAR 31.205-45 .

1.1.5 Hours of Operations and Recognized Holidays

The contractor is responsible for performing during normal business hours (i.e. 8:00am to 5:00pm), except on Federal Holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closures. A list of Federally recognized Holidays is below:

New Year's Day	Labor Day
Juneteenth Day	Martin Luther King's Birthday
Columbus Day	President's Day
Veterans Day	Memorial Day
Thanksgiving Day	Independence Day
Christmas Day	

Mission support requires that there is an on-call capability during these Federal Holidays and other approved / recognized closures.

1.1.6 Standards: The contractor must adhere to all DOD, Defense Information Systems Agency (DISA), Army, and AAG specific enterprise architecture standards. Changes in

hardware or software configurations only occur with advanced AAG Infrastructure Configuration Control Board's (ICCB) approval. If an environmental change is introduced, it must be seamless, with a risk-mitigated transition plan , that will minimize the impact to AAG's customers performed in accordance with AAG Change Management Procedures, AAG Problem Management Procedures, Standard Operation Procedures, applicable, DISA, DOD, and Army policy and regulation, and other applicable AAG procedures and plans as applicable.

1.1.7 Contractor Manpower Reporting (CMR): The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.SAM.gov

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2025.

1.1.8 Personnel: The contractor shall provide IT2 Level Certified personnel IAW DOD 8140.03 within 30 calendar days of award and backfill any subsequent vacancy within 30 calendar days.

Contractor personnel shall Obtain/Maintain a favorably adjudicated Secret clearance when required prior to beginning work under this contract (Determined by a review of each individual's DISS file). Personnel will either submit for a T3 background investigation or have a favorably adjudicated T3 (or equivalent) on file in DISS prior to beginning work under this contract. If at any time, any contractor person is unable to obtain/maintain a favorably adjudicated T3 or equivalent, the contractor person shall be immediately removed from work under this contract and the Government site.

2. Security Requirements

2.1 Security Program: All contractor personnel performing under this contract must possess and maintain a current SECRET security clearance. Security clearances are required prior to personnel commencing work. Interim security clearance maybe considered on a case-by-case basis as approved by the COR and contracting officer. Security requirements shall be in accordance with DD Form 254, Contract Security Classification Specification (Attachment xxxxx) .

2.1.2 Security Clearance and Data Access: Contractor personnel may have access to classified and sensitive but unclassified information. In the event the contractor is given access to classified and sensitive Government data, the contractor hereby agrees to protect such data from unauthorized use or disclosure as long as such data remains classified and/or sensitive. In order to protect this classified and/or sensitive information,

the contractor shall comply with DOD Manual 5200.01 (Volumes 1-3), DoD Information Security Program, DOD Manual 5200.02 (DoD Personnel Security Program), and AR 380-67 (U.S. Army Personnel Security Program).

2.1.3 Non-Disclosure Agreements: Performance under this contract may require the Contractor to access data and information proprietary to a Government agency, another Government Contractor, or of such nature that its dissemination or use other than as specified in this work statement would be against the interests of the Government or others. The Contractor and Contractor personnel shall not divulge, or release data or information developed, or obtained under performance of this PWS, except to authorized Government personnel or upon written approval of the Contracting Officer. The Contractor shall not use, disclose, or reproduce proprietary data, which bears a restrictive legend, other than as specified in this PWS. All documentation showing individual names or other personal information shall be controlled and protected under the provisions of the Privacy Act of 1974, Public Law 93-579, 5 United States Code (U.S.C.) Section 552a.

2.1.4 Non-Disclosure Statements: The Contractor shall provide signed non-disclosure agreements to the Government prior to commencement of work under the contract. Disclosure of information by Contractor personnel may result in removal of Contractor personnel from performance under this contract. The contractor should refer to DOD Manual 5200.02, Personnel Security Program for details; all contractor personnel shall also sign or already have on file in DISS a Classified Information Nondisclosure Agreement (Standard Form 312).

2.1.5 Organizational Conflict of Interest (OCI): Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent OCI as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI (*{Insert Deliverable #}*). The Contractor's OCI Mitigation Plan will be determined to be acceptable solely at the discretion of the Contracting Officer. In the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

2.1.6 Installation Access: Access to U.S. installations, buildings and controlled areas is limited to personnel who meet security criteria and are authorized. Failure to submit required information/data and obtain required documentation or clearances will be grounds for denying access to U.S. installations, buildings and controlled areas. The Contractor shall ensure that any subcontractors used in performance of this contract

complies with these requirements and that all employees, of both the Contractor and any subcontractor utilized by the Contractor, are made aware of and comply with these requirements.

2.1.6.1 The Contractor shall be aware of and comply with the requirements associated with Installation Access Control. The Government is not liable for any costs associated with performance delays due solely to a firm's failure to comply with Installation Access Control System (IACS) processing requirements.

2.1.6.2 The Contractor shall return installation passes to the issuing IACS office when the contract is completed or when a Contractor employee no longer requires access.

2.1.7 Common Access Card (CAC): Contractor personnel requiring access to Government facilities or have a need to access Government networks shall obtain/wear Government-issued access badges (Common Access Card). While in Government facilities, the CAC shall be worn above the waist, or in accordance with local policy.

2.1.7.1 The contractor shall be required to access Communications Security (COMSEC) information, Non-Special Compartmentalized Information (SCI), and Controlled Unclassified Information (CUI). The contractor shall also be required to access Secret Internet Protocol Router Network (SIPRNET) at Government facilities only. Tempest requirement is applicable (DI-EMCS-81684, TEMPEST Test Evaluation Report). The contractor shall comply with all applicable government security clearance regulations and procedures contained in DoD 8140.01, DoD 8140.02, DoD 8140.03, AR 25-2, and DoD 8500-2.

2.1.7.2 Contractor personnel requiring COMSEC access must be U.S. citizens and possess a final clearance at the appropriate level. All contractors shall be briefed before access to COMSEC is granted. The contractor shall require a COMSEC account and perform Automated Information System (AIS) Processing In Accordance With (IAW) CDRL A0002 (DI-MGMT-80934C), Operation Security (OPSEC) Plan. The contractor shall receive classified information only at another contractor's facility or a Government facility.

2.1.7.3 All contractor personnel shall execute a DD Form 2841, Department of Defense (DOD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities and adhere to the acknowledged responsibilities there under (required for CAC issuance).

2.1.7.4 All contractor personnel shall complete initial and annual AAG Information Assurance (IA)/Security Awareness (SA) training and other security related training provided by AAG to ensure users understands all AAG, DISA, DOD and Army protocols. Selected tasks under this contract will require contractor personnel to obtain/maintain personnel security clearances at a minimum of SECRET level, depending upon the classification of the materials to be accessed. This requirement is identified in the tasks,

accordingly. The contractor must maintain a database of all IA/SA training documents for everyone who has access to the AAG enterprise system.

2.1.7.5 All contractor personnel under this contract shall comply with AAG Information Systems Security procedures to obtain proper security clearance or vetting prior to beginning work under the contract. Based upon the work to be performed under the contract, the AAG Information Assurance Manager (IAM) will determine the proper vetting or security clearance requirement. Due to varying access requirements, information and data to which each contractor person may have access, personnel security clearance and vetting requirements will vary.

2.1.8 Data Access

2.1.8.1 All contractor personnel supporting this PWS who require access to Government Information Systems are required to receive and complete; initial Information Assurance (IA) orientation awareness training before being granted access to the system(s) and annual IA awareness training to retain access, as required DoD 8140, and DODI 8500.01.

2.1.8.2 The contractor shall provide all Information Assurance Certificates to the Government prior to gaining access to the Government network.

2.1.8.3 As a “condition of employment” the contractor personnel must obtain and maintain currency for appropriate certification(s) required for the position IAW DoD 8140.03. Paragraph 3.2., DoD Cyberspace Workforce Qualification and Management Program.

2.1.8.4 Agency-approved IA workforce certifications appropriate for each category and level as listed in the current version of DoD 8140.03.

2.1.8.5 Appropriate operating environment certification for IA technical positions as required by the Government IAW DoD 8140.03.

2.1.8.6 The contractor shall provide documentation supporting the certification status of personnel performing IT functions. Certification must be current and specific to the system they manage (i.e. SQL, Oracle, Citrix, etc.)

2.1.8.7 Contractor personnel who do not have proper and current certifications will be denied access to Government information systems for the purpose of performing IT functions.

2.1.9 Antiterrorism / Operations Security

2.1.9.1 Antiterrorism (AT) Level I Training: All contractor employees, to include subcontractor employees, requiring access to government installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar

days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: https://jkodirect.jten.mil/pdf/atl1/launch.html

2.1.10 AT Awareness Training for contractor Personnel Traveling Overseas. This standard language text required US based contractor employees and associated sub-contractor employees to make available and to receive government provided area of responsibility (AOR) specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander with the unit ATO being the local point of contact.

2.1.11 iWATCH Training. The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

2.1.12 Access and General Protection/Security Policy and Procedures. Contractor and all associated sub-contractors' employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. In addition to the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

2.1.12.1 Contractor and all associated sub-contractors' employees shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with "(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

2.1.12.2 The contractor shall develop an Operations Security (OPSEC) Standing Operating Procedure (SOP)/Plan (CDRL A0002, DI-MGMT-80934C) within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan will include the

government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. The contractor will ensure this individual becomes OPSEC Level II certified per AR 530-1.

2.1.13 OPSEC Training: Per AR 530-1, Operations Security, new contractor employees must complete Level I OPSEC training within 30 calendar days of their reporting for duty. All contractor employees must complete annual OPSEC awareness training. OPSEC Awareness training can be found at https://securityawareness.usalearning.gov/opsec/index.htm

2.1.14 Information Assurance (IA) Training: All contractor employees who require access to a government information system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.

2.1.14.1 All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working in IA/IT functions must comply with DoD and Army training requirements in DoDD 8140.01 and AR 25-2 at the start of employment.

2.1.14.2 Per DoDD 8140.01, DFARS 252.239.7001, and AR 25-2, all contractor employees supporting IA/IT functions shall be appropriately certified before contract award. The baseline certification as stipulated in DoD DoDD 8140.01 must be completed before contract award.

2.1.14.3 Per AR 381-12, Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b of AR 381-12.

2.1.15 Facility Security: The facility security requirements are defined in DD Form 254, Contract Security Classification Specification. The highest level of facility clearance required for the contractor to perform on this task Order is SECRET. contractor must have SECRET clearance at the time of award and must maintain clearance throughout the contract at contractor expense. Clearance level may be updated later via a modification to the DD254.

- The highest level of classified material the contractor will be required to safeguard at its own facility is NONE.
- This Contract will require access to CUI INFORMATION.
- This Contract will require access to Protected Health Information (PHI) and Personally Identifiable Information (PII).
- In performing this contract, the contractor will perform services only.

- In performing this contract, the contractor will have operational security (OPSEC) requirements.
- In performing this contract, the contractor will require sensitive IT duties.

2.2 Purchasing of Software and Information Technology equipment.

2.2.1 The contractor shall support all Government and contractor procured IT hardware and software purchases required to support this contract. All hardware and software must follow Industry Best Standard using independent industry analyst (i.e. Gartner). The hardware and software must meet all applicable DISA, DoD, and Army regulations for use on the network. The contractor shall use this hardware and software to support all requirements listed in PWS Section 3. For Other Direct Cost (ODC) purchases, the contractor shall request and receive written approval from the Contracting Officer's Representative (COR) prior to purchasing any hardware or software as an ODC. All hardware/software purchases must meet the Army Computer Hardware, Enterprise Software and Solutions (CHESS) program requirements to include ordering equipment through the Information Technology Enterprise Solutions (ITES) ordering system. The CHESS program website is www.chess.army.mil. The contractor shall provide the Contracting Officer and COR a copy of all completed invoices prior to invoicing against Contract Line Item as soon as possible following the purchase. If item is not found in CHESS, vendor will submit a Statement of Non-Availability.

2.2.2 Comply with Section 508 capability requirements that require federal agencies' electronic and information technology is accessible to people with disabilities.

2.2.3 Purchases will be completed within ten (10) duty days and invoiced within two (2) months. The contractor shall inform the COR of any issues or problems associated with purchasing the items on a weekly basis.

2.3 Quality Control Plan (QCP):

2.3.1 The Contractor shall develop and maintain a QCP to ensure services are performed in accordance with (IAW) this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's QCP is the means by which it assures that the work provided complies with the requirements of the contract.

2.3.2 The Contractor's Proposed QCP shall be submitted to the Contracting Officer (KO) through the Contracting Officer's Representative (COR) for review within (Insert # of Days) after date of contract award.

2.3.3 The Contractor shall develop and maintain a QCP to ensure services are performed in accordance with (IAW) this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's QCP is the means by which it assures that the work provided complies with the requirements of the contract.

2.3.4 The Contractor's Proposed QCP shall be submitted to the Contracting Officer (KO) through the Contracting Officer's Representative (COR) for review within (Insert # of Days) after date of contract award.

2.3.5 The Government will review and either notify the Contractor in writing of acceptance of the plan or return their comments to the Contractor within *(Insert number of days)*. If the Government has provided comments, the Contractor shall then have *(Insert number of days)* to submit a Final QCP. After receipt of the Final QCP, the Contractor may receive the Contracting Officer's acceptance in writing. Any proposed changes to the accepted QCP are required to be resubmitted for acceptance by the Contracting Officer no later than *(Insert number of days)* prior to the anticipated change and before implementation by the Contractor. The timeline noted above will apply for review and acceptance for proposed changes. At a minimum, the QCP must include and answer the following to be acceptable:

(a) A chart showing the organizational structure and lines of authority, the names, qualifications, duties, responsibilities, and classification of each member of the Contractor's Quality Control Team;

(b) How the Contractor will monitor work to ensure performance complies with all deliverables (etc. timelines, deadlines, and goals);

(c) How the Contractor will monitor work to ensure performance complies with all specifications and requirements of the contract, including the contract's clauses;

(d) How the Contractor will monitor and ensure staff qualifications remain current and valid including Department of Defense (DoD) Contractor Personnel Office (DOCPER) processes/approvals throughout contract performance;

(e) How the Contractor will ensure all keys issued will remain controlled items (Paragraph 1.7 Key Control);

(f) How the Contractor will inventory and track maintenance of all Government Provided Equipment / Materials;

(g) How the Contractor will identify, investigate, and correct any non-conforming performance and prevent similar deficiencies in the future; and

(h) How the Contractor will file and save all Quality Control related documents for the life of the contract plus 5 years.

2.4 Quality Assurance: The Government will evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how

the performance standards will be applied, the frequency of surveillance, and the acceptable quality levels (performance thresholds).

3.0 Requirements

3.1 Scope: Contractor shall provide support services to Army Analytics Group (AAG) for Development Security Operations, Hosting, & Software Support (DevSecOps) in the following areas software maintenance and enhancements for AAG supported applications.

- Data Integration and Transformation services for AAG supported applications
- Provide Security Code Scanning and documentation for AAG managed applications
- Provide quality assurance supporting data integration and transformation services for AAG managed applications
- Provide Configuration and Change management services for AAG managed applications
- Provide Development and Operations services supporting continued integration and continuous delivery of software for AAG managed applications
- Desktop Administration
- Network Support and Infrastructure for Operational Server Support
- IT Asset Management
- Operations Project Management
- Database Support, and Systems Support
- Operations Configuration Management
- Operations Change Management
- Incident Analysis
- Cloud hosting and engineering

These tasks must use practices, such as Lean, Agile, and DevSecOps that focus on rapid, iterative development and delivery of software with active user engagements. Small cross-functional software development teams integrate planning, design, development, testing, security, delivery, and operations with continuous improvement to maximize automation and user value. (DoDI 5000.87)

The Government shall evaluate the contractor’s performance under this contract in accordance with Table 1 – Service Metrics, and Table 2 – Performance Requirements Summary, below. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

INSERT TABLE HERE

3.2 Phase-In: The contractor shall be responsible for providing a Phase-In plan conducting all tasks necessary to be capable of fully performing within 60 days after contract award without disruption or degradation of the mission (CDRL A0008 DI-SESS-82299, . The contractor is responsible for coordination of all information needed to obtain appropriate access to facilities and the badges required by government sites. Contractor Phase-In tasks include ensuring that sufficient resources that are fully trained and qualified to perform the requirements set forth in the PWS are on hand and available to begin work on contract start date.

3.3 Phase-Out: The contractor shall submit a phase-out plan, which enables a smooth transition to replacement services for 30 days prior to the end of the Period of Performance (including technical data rights considerations). A Phase-Out plan will be required to be delivered 30 days after contract award. If time allows the phase out will occur during the 30 days after new award is made, but no earlier than 30 days prior to the end of this contract. The contractor shall ensure there will be no service degradation during the transition. Services will include supporting all items listed in paragraph 3.1 and provide an orderly turn-over of responsibilities. The plan shall provide support for up to 30 days to the selected contractor if the incumbent contractor is not selected for a subsequent contract. contractor is responsible ensuring all required documentation to maintain the network is provided to new contractor. contractor will not destroy documents (certificates, whitelist, IP list, architecture drawings, passwords (locked in safes), and password wallets needed for continuity. The contractor is responsible for returning all badges and access obtained as a result of performance under the contract. contractor Phase-out tasks include ensuring that sufficient resources are available to perform the requirements set forth in the PWS during the 30-day Phase-out period.

3.4 Surge Requirements

This contract may require the contractor to provide additional support to application access, increase network security requirements, enhance web interfaces, dashboards, web pages, database management for logistics, financial, personnel tracking, accounting, evaluating, and data analysis as required. The projects require the same skill sets as established by this PWS. Work will be conducted as a Firm Fixed Price due to the time constraints and nature of the requirement. AAG anticipates special, time sensitive projects based on historical records yearly. Additionally, mandated security requirement upgrades & network inspection will require increase level of effort. Additional level of effort will be required for preparation before inspections as well as the actual inspections. As the number of networks increase, the number of network inspections will increase. This includes no notice inspections that will be required over above the normal workload. The contractor shall support increased workload as needed to meet mission requirements as directed and approved by the by AAG Contracting

Officer's Representative (COR). Rates for the Surge CLIN will be the same as those listed in the main labor CLIN of the proposal. This surge support is limited to the funding provided on contract on the surge CLIN and the contractor shall not work and bill for hours above the funded amount on contract.

3.5 Postproduction Software Support Services (PPSS)

3.5.1 The contractor shall analyze software enhancement and modification requests to assess impact and feasibility and recommended action. Final recommended action shall be documented IAW CDRL A0026, DI-MISC-81807, Software Change Request (SCR).

3.5.2 The contractor shall implement approved SCRs. This includes design of the recommended solution, coding to the design, and ensuring the modification meets the required need for the modified software IAW CDRL A0027, DI-IPSC-81427B, Software Development Plan.

3.5.3 The contractor shall update and keep current all system and software documentation to reflect implemented changes and ensure that all revised documentation is logged and stored in a Government-specified database or repository. Submit in IAW CDRL A0006 (DI-IPSC-81756, Software Documentation).

3 5.4 The contractor shall ensure that all source code, executables, data sets, installation scripts, configuration files and other software used and developed by the contractor for system/software engineering is stored in a Government-specified database or repository. Submit software/source code (CDRL A0019, DI-IPSC-81441A, Software Product Specifications).

3.5.5 The contractor shall produce software release packages, which include all software required to install the release on target system(s), all end user documentation and release notes (CDRL A0028, DI-IPSC-81428A, Software Installation Plan). For major releases only, the end user documentation shall include a Software Version Description Document (CDRL A0020, DI-IPSC-81442A, Software Version Description (SVD)).

3.5.6 The contractor shall plan and conduct functional testing of software for each release to ensure compliance with documented functional requirements specification. Functional requirements specification will be provided as Government-furnished information IAW CDRL A0029 and A0030 (DI-IPSC-81438A, Software Test Plan and DI-IPSC-81440A, Software Test Report).

3.5.7 The contractor shall ensure all software complies with applicable DISA Security Technical Implementation Guides (STIGs), Army Cyber Command (ARCYBER) Operations Orders (OPORDs) and Army and DoD Best Business Practices (BBP).

3.5.8 The contractor shall maintain all software to meet requirements of AR 25-2 Information Assurance, DODD 8500.1 Information Assurance and DODI 8500.2 Information Assurance Implementation.

3.5.9 The contractor shall ensure software changes meet requirements sufficient to maintain existing Authority to Operate (ATO) as determined by the Department of Defense Information Risk Management Framework.

3.5.10 The contractor shall assist the development and review of the Plan of Action & Milestones (POA&M) and RMF package. POA&Ms are generated quarterly or when RMF accreditation is required to include packages for cloud platforms.

3.6 Maintenance of Software

3.6.1 The contractor shall provide maintenance software patches for configuration board approved bug fixes, information assurance vulnerability fixes, and software fixes for performance tuning.

3.6.2 The contractor shall provide maintenance software patches for configuration board approved minor change requests due to changes in policy and directives.

3.6.3 The contractor will perform a scan of new and enhanced applications for security and quality assurance testing before each release to production servers IAW AAG Application Software Assurance Scan, CDRL A0031 (DI-IPSC-82249A, Software Assurance Evaluation Report)

3.6.4 The contractor shall analyze software enhancement and modification requests to assess impact and feasibility and recommended action.

3.7 Code Scanning

3.7.1 The contractor will perform a scan of new and enhanced applications for security and quality assurance testing before each release to production servers IAW AAG Application Software Assurance Scan.

3.7.2 The contractor will compile the results and report risk, security exposures, vulnerabilities, and noncompliance of applications that were tested after each scan.

3.7.3 The contractor will use a variety of IA tools to perform code scanning, web scanning, and fuzz testing on applications managed by AAG.

3.7.4 The contractor will provide Software Test Procedures, successfully verify and validate conformance with functional requirements specifications.

3.7.5 The contractor will provide a monthly Software Test Report (DI-IPSC-81440A)

3.7.6 The contractor shall validate that there are no outstanding category 1 or 2 software anomalies or documentation issues with released software

3.7.7 The contractor shall ensure all software complies with applicable Defense Information Systems Agency (DISA), Army Cyber Command (ARCYBER) Operations Orders (OPORDs) and Army , DoD, and commercial Best Business Practices.

3.7.8 The contractor shall ensure software meets requirements of AR 25-2 Information Assurance, DODD 8500.1 Information Assurance and DODI 8500.2 Information Assurance Implementation.

3.7.9 The contractor shall test and validate all software updates for security compliance and support the Government for security related issues on the software. Examples of support include providing information on status of IAVMs and providing information in support of system/software/facility accreditation.

3.7.10 The contractor shall test and validate all software updates for security compliance and support the Government for security related issues on the software.

3.7.11 The contractor will provide written scan results within one day after completion of the test scan via ticketing system.

3.8 Configuration Management Support

Objective: Track the submission, coordination, review, evaluation, categorization, and approval for release of all changes to the AAG portfolio's software configuration baselines.

3.8.1 The contractor shall maintain configuration control of approved software versions and documentation IAW Attachment 4 "AAG Software Configuration Management Plan (SCMP)." All Change request shall be submitted to the Application Configuration Control Board (ACCB)

3.8.2 The contractor shall maintain configuration control of all products under development IAW Attachment 4 "AAG Software Configuration Management Plan (SCMP)."

3.8.3 The contractor shall support configuration audits IAW Attachment 4 "AAG Software Configuration Management Plan (SCMP)."

3.8.4 The contractor shall track and maintain a list of change requests and task completions of tickets for the Configuration Management system.

3.8.5 The contractor shall update software version description document and data dictionary upon completed of all change request.

3.9 Data Management Support

Objective: Accumulate, transform, and access control personnel, financial, and logistic related data for research studies and projects.

3.9.1 Contractor shall conduct data acquisition and transformation to include Extract, Transform, and Load (ETL), data cleansing, data catalog updates and data quality to ensure the data is fit for use. Provide a Data Dictionary in the Computer Software Product End Item (CDRL A0021, DI-ACVS-80700A) for each transformed data set. Deliver automated scripts used for data transformation.

3.9.2 Contractor shall prepare Data Usage and Sharing Agreements that specify the intent, practice, and limits of data sharing between data providers and data consumers Data Usage and Sharing Agreement (A0027, DI-MISC-80508B, Technical Report: Study/Services).

3.9.3 Contractor shall provide expertise in medical data extraction, load, and transfer (ETL) operations to ensure compliance with the 1996 Health Insurance Portability and Accountability Act (HIPAA) for handling Protected Health Information (PHI).

3.9.4 Contractor shall possess expertise in statistical analysis of large datasets and sampling techniques for surveillance of Personal Identifiable Information (PII) and an expert level knowledge of de-identification procedures and methods.

3.9.5 Contractor shall provide expert level working experience with the TRICARE Management Authority Medical Health System Medical Data Repository, the MODS Periodic Health Assessment, and Deployment Health Assessment Program data assets.

3.9.6 Contractor must be skilled in large data mining including Oracle, PL/SQL, Microsoft SQL Server, T-SQL, PostgreSQL, Microsoft .NET, Python, SQL, SAS and other commercial relational and database programming languages to include but not limited to Big Data Platform.

3.10 Training Support

Objective: Provide User level training for the AAG portfolio software.

3.10.1 The contractor shall develop and provide training material for local administrators and users in the format of CDRL A0026, DI-MGMT-81605, Briefing Materials.

3.10.2 The contractor shall provide web base user training via Government provided web conferencing tool. (i.e., Defense Collaboration Services [DCS])

3.11 Program Management

Objective: Conduct project management to control cost, schedule and performance for all work under this contract

3.11.1 The contractor shall attend project meetings, respond to technical questions, and address requests for information (CDRL A0017, DI-ADMN-81308A, Conference Report).

3.11.2 The contractor shall submit monthly performance and cost report (DI-FNCL-80912, Performance and Cost Report).

3.11.3 The contractor shall submit monthly funds & manpower report (CDRL A0019, DI-FNCL-80331A) Funds & Manhour Expenditure Report.

3.11.4 The contractor shall submit monthly status report (CDRL A0005, DI-MGMT-81928, Contractor's Progress and Status Report).

3.11.5 The contractor shall provide 100% qualified personnel within 30 calendar days of award and backfill subsequent vacancy within 30 calendar days.

3.11.6 The contractor shall complete all Government mandated training requirements as determined by AAG for contractor employees that occur during the period of performance of this contract. In addition, HIPPA training will be completed by the contractor as required by Attachment 5 "AAG Special Training" and Attachment 6 "AAG Special Training HIPPA Statement."

3.12 Cloud Migration

3.12.1 Provide expertise in developing the creation of Templates, Documentation, and a Roadmap and conducting assessments to assist AAG with identifying which applications are appropriate candidates for cloud migration.

3.12.2 Prepare the identified applications for cloud migration. This shall include, but not be limited to the development of checklist and process Documentation that can facilitate AAG in preparing for migration.

3.12.3 Assist AAG and AAG partners in migrating applications to and from the cloud. This shall include, but not be limited to the use of best practices to test and subsequently migrate applications to take advantage of the cloud.

3.12.4 Assist AAG customers in the administration, maintenance, and support of applications in the cloud and AAG's hybrid cloud.

3.13 Data Rights

3.13.1 The Government's rights in non-commercial technical data and software deliverables shall be governed by DFARS 252.227-7013 and DFARS 252.227-7014, respectively. Pursuant to the requirements set forth in DFARS 252.2277017, Offerors are required to specifically identify Data/Software Rights Assertions related to technical data and software deliverables. As indicated in DFARS 252.227-7017(e), an Offeror's failure to submit, complete, or sign the aforementioned Data and Software Rights Assertions with its offer may render the offer ineligible for award.

3.13.2 The Government will retain full, unrestricted, unlimited rights to all data produced in the course of contract performance. Deliverables containing information proprietary to the contractor shall prominently display the legend "Proprietary to (contractor Name)". In the event that the Government identifies a need to provide one or more deliverables to other contractors, the contractor shall provide a releasable document that does not bear the proprietary legend within 2 hours of a Government request. Data that does not bear the proprietary legend shall be

4. Hosting & Infrastructure: Hosting and infrastructure will consist of the utilization of CI/CD pipeline deployment of code as infrastructure. The utilization of Agile methodologies shall be used to manage this portion of the work.

4.1 Workstation & Laptop Administration

4.1.1 The contractor shall assist/maintain government-provided 25 physical laptops and/or workstations, physical, virtual desktops, and mobile devices, to provide optimal performance and availability.

4.1.2 Monthly results are reported in the IT Asset Inventory (CDRL A0001, DI-MGMT-80442, Report of Receipts, Inventory, Adjustments, and Shipments of Government Property). The contractor shall conduct an annual inventory to cover all assets. A monthly inventory will cover successive 10% portions of the inventory.

4.1.3 The contractor shall inventory, deploy, retrieve, and upgrade workstation and peripherals to support contractor personnel changes and life-cycle upgrades.

4.1.4 The contractor shall troubleshoot and resolve virtual hardware and software workstation related incidents as required within timelines per ticket severity and provide an Incident Response Report for issues outside of normal duty hours to be provided in the monthly status report (CDRL A0003, DI-MGMT-80368A, Status Report).

4.1.5 The contractor shall make recommendation for upgrades and improvements support performance issues and comply with life-cycle asset management.

4.1.6 The contractor shall maintain a 100% accurate inventory and archive historical data on all systems to include Wisetrack (other designated inventory system), the Army inventory system, and other tracking software as directed by the government. The contractor shall dispose of all end-of-life cycle and outdated systems IAW DOD Army regulations and AAG operating procedures.

4.1.7 The contractor shall integrate new workstation technologies to include hardware and software changes IAW DoD, DISA, Army and AAG regulations and policies.

4.1.8 The contractor shall identify and provide operational support for all network printers, scanners, copiers, and other peripheral equipment to ensure best performance and availability.

4.2 Software Support

4.2.1 The contractor shall maintain an end user application catalog comprised of all software (DI-AVCS-80700A) approved for implementation on AAG user platforms. The catalog shall include the Assess Only number, the title of the software, manufacturer, and number of approved licenses and version of the approved software packages. Current software is listed in (Attachment E – virtual Hardware & Software Listing).

4.2.2 The contractor shall maintain original and backup copies of all software. Additionally, the contractor will also maintain the current license list as well as the keys.

4.2.3 The contractor shall notify the COR in writing when license thresholds are reached on all systems.

4.2.4 The contractor shall notify the COR, in writing, 3 months prior to the software version will reach end of support date or expiration date.

4.2.5 The contractor shall create installation packages for software automated installations in line with the new CIO policy directive.

4.2.6 Integrate/maintain new application streaming and application virtualization technologies

4.3 Network Support and Infrastructure

4.3.1 Enterprise Network Monitoring

4.3.1.1 The contractor shall monitor and report on the overall health of the network and system infrastructure with the Application/Network Downtime Critique Reports (CDRL A0004, DI-MGMT-80368A, Status Report), to include equipment attached to the network and all applications also running over the network directly supporting the network.

4.3.1.2 The contractor shall respond to outages reported through the Azure DevOps ticket process (Performance Requirement Summary & Service Metrics Table 1 & 2) within timelines per reported outage severity. The contractor shall provide On Call and Response Reports for each of the Azure DevOps tickets (CDRL A0015, DI-MISC-80279A, Utilities Outage and Status Report).

4.3.2 Network Device Administration

4.3.2.1 The contractor shall maintain all enterprise network infrastructure resources and services for all AAG environments ensuring optimum performance and availability. The contractor shall install, configure, and maintain network equipment, to include a combination of network routers, Intrusion Prevention Software (IPS), Intrusion Detection Software (IDS), switched, and firewalls per (Attachment E – Virtual Hardware & Software Listing).

4.3.2.2 The contractor shall perform all network device administrative functions. All network scheduled outages shall be pre-approved by the Infrastructure Change Control Board (ICCB) as authorized outages.

4.3.2.3 The contractor shall ensure proper LAN and server cabling to comply with Electronic Industries Alliance (EIA)/Telecommunication Industry Association (TIA) standards and all national/federal standards

4.3.2.4 The contractor shall support the government-owned firewalls and routers at its facility. In performing infrastructure, operational and maintenance functions, the contractor shall follow the security and operational regulations of appropriate government agencies. The contractor shall troubleshoot and coordinate fix actions with appropriate agencies to resolve all LAN/WAN issues.

4.3.2.5 The contractor shall respond to outages reported through the Azure DevOps ticket process within the timeframes for reported network issues and outage severity (CDRL A0015, DI-MISC-80279A, Utilities Outage and Status Report).

4.3.3 Network Infrastructure Integration Support

4.3.3.1 The contractor shall ensure that a combined network switches, routers, firewalls, either virtual or physical, are integrated and operate in accordance with DISA, DoD,

Army, commercial standards, and federal policy performance standards. Every effort must be taken to ensure the maximum amount of operational availability of the network services is experienced.

4.3.3.2 The contractor shall develop for approval implementation plans for continual availability improvements for the network services (DI-MISC-80919 DI-SESS-81625). The plans must be approved by the ICCB.

4.3.3.3 The contractor shall track change management activities that impact network administration functions. All integration efforts must adhere to security and operational parameters and constraints existing at the time the integration is required.

4.3.3.4 The contractor shall maintain a local and long-haul list of circuits and infrastructure architectural drawings of all configurations and diagram all circuits (MIL-STD-2045). The list will be maintained in the current ARMY collaboration suite, for example A365.

4.3.3.5 The contractor shall respond to outages and changes reported through the Azure DevOps ticket process within (Performance Requirement Summary & Service Metrics Table 1 & 2) timelines per reported outage severity. The contractor shall make changes only as received through approved Azure DevOps tickets.

4.3.3.6 The contractor is to develop, with input from Government approved vendors, network baseline architecture documentation.

4.3.3.7 The contractor shall manage and maintain approved Domain Name System (DNS), Ports Protocols and Services (PPS), and Whitelist of all AAG managed applications.

4.3.3.8 The contractor shall manage and maintain circuit accountability.

4.3.3.9 The contractor is responsible for updating the baseline network architecture when changes are made.

4.3.4 Troubleshooting and Technical Support Duties

The contractor shall identify problem areas, propose a potential workaround and then implement effective solutions in a manner that restores the availability of the AAG services. Typical work includes functional analysis, technical analysis, network capture and analysis, and service restoration.

4.3.5 Configuration Management

The contractor shall incorporate AAG-approved enhancements, improvements and modifications to the AAG physical and virtual network resources to prevent the loss of services due to conflicting changes, allow full visibility of the proposed work and provide an ability to view the changes potential impact on resulting resources, services and customers. The contractor shall use AAG's Network Configuration Management tool to the maximum extent possible.

4.3.6 Configuration Baseline Changes

4.3.6.1 The contractor shall review changes and perform audits periodically to ensure only authorized changes are implemented. Examples of change orders include Urgent Configuration Changes to be performed within one (1) calendar day, Routine Configuration Changes to be performed within seven (7) calendar days, or in the time directed by DISA, DoD, and other entities such as Army Cyber Command, NETCOM and other various agencies.

4.3.6.2 The contractor shall ensure that AAG's enterprise resources and assets are protected against all potential threats and vulnerabilities.

4.3.6.3 The contractor shall ensure the AAG Enterprise applications and projects functions perform at optimum levels and availability, ensuring strict adherence to all applicable Information Assurance Vulnerability Alerts (IAVA's), Security Technical Implementation Guide's (STIG's), Assured Compliance Assessment Solution (ACAS), and industry best practices. The contractor shall create and maintain network infrastructure device rules and conduct configuration reviews as appropriate and approved by the Configuration Control Board (CCB).

4.3.6.4 The contractor shall audit all system logs, and ensure logs are backed up and included in the Security Identification Event Management (SIEM) infrastructure.

4.3.6.5 The contractor shall implement and maintain security configurations for all AAG enterprise network assets and configurations. All security configurations and operations must be IAW the DODI 8500.2 and compliant with any additional DOD Instructions, Federal Information Security Management Act (FISMA) Army and AAG policies. The contractor shall use the AAG's Network Configuration Management tool to the maximum extent possible.

4.4 Network Monitoring and Report Generation

4.4.1 The contractor shall provide continuous, accurate assessments of the current and projected health of the overall AAG Network Infrastructure.

4.4.1 The contractor shall provide continuous and accurate assessments of AAGs available resources ensuring the AAG Enterprise applications projects function at

optimum performance levels, and availability initiating necessary actions to resolve noted areas of concerns and deficiencies. The contractor shall configure network alerting, monitor and respond to alert messages, monitor available network infrastructure resources and perform capacity analysis.

4.4.2 The contractor shall ensure that all Government approved cloud native components are integrated and operate in accordance with performance standards. Every effort must be taken to ensure operational availability of the network services.

4.4.3 The contractor shall develop and present for approval and implementation, plans for continual availability improvements for the network services. The contractor shall track change management activities that impact network administration functions. All integration efforts must adhere to security and operational parameters and constraints existing at the time the integration.

4.5 Operational Server Support: The contractor shall provide complete lifecycle support for all AAG enterprise servers and services in unclassified and classified environments to ensure they maintain optimal performance, and capabilities in accordance with established DOD and AAG policies.

4.6 Domain/Enterprise Service

4.6.1 The contractor shall maintain up to 10,000 user accounts within the enterprise, including creating, deleting, disabling, granting access to resources and changing account properties. Historically fewer than 10% require monthly action.

4.6.2 The contractor shall provision all accounts for authorization and authentication.

4.6.3 The contractor shall maintain all network services required within the enterprise, including but not limited to: Secure Shell (SSH), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), Secure File Transfer Protocol (SFTP), DNS, Dynamic Host Configuration Protocol (DHCP), Group Policy, and Lightweight Directory Access Protocol (LDAP).

4.6.4 The contractor shall maintain all security and distribution groups, create new groups as requested, and manage group membership and group access control.

4.6.5 The contractor shall maintain Online Certificate Status Protocol for certificate verification and revocation services.

4.6.6 The contractor shall respond to Domain/Enterprise Service Azure DevOps within (Performance Requirement Summary & Service Metrics Table 1 & 2 timelines per reported Azure DevOps severity.

4.7 Operating System and Hardware Services

4.7.1 The contractor shall maintain all virtual server operating systems to ensure latest patching/security updates are applied to all environments. Patching of hosted applications in all AAG managed enclaves.

4.7.2 The contractor shall maintain all server environments for maximum health and availability to include operating systems, installed software, and hardware.

4.7.3 The contractor shall install software on servers as required by the government.

4.7.4 The contractor shall maintain base images of all server operating systems, both for physical and virtual installations.

4.7.5 The contractor shall maintain lifecycle management for all Operating System (OS) versions.

4.7.6 The contractor shall maintain lifecycle management for all hardware platforms to include end to life support, such as preparing equipment for disposal and removal of equipment from the government property books (Wisetrack and PBOS).

4.7.7 The contractor shall maintain Laws Regulation and policies of consistency for DISA, DoD, and Army standards of operating systems used within the enterprise.

4.7.8 The contractor shall format, configure, and deploy new servers based upon requirements IAW DoD, DISA, Army, and AAG regulations.

4.7.9 The contractor shall update virtual or physical hardware with the latest firmware versions within 28 days of Government.

4.8 Monitoring Services

4.8.1 The contractor shall maintain a monitoring system that will report the overall health of all servers, applications, and devices in the enterprise.

4.8.2 The contractor shall assist with creating and maintain a solution for viewing for viewing live system statuses.

4.8.3 The contractor shall maintain and use an alerting system for Government and contractor personnel in the event of an outage.

4.9 Data Backup, Retention and Recovery

4.9.1 The contractor shall backup all data on all production, development, and test servers with all source codes at AAG. Additionally, file shares and databases as required and maintain backups per AAG SOP-OPS-16, SOP-OPS-17, and SOP-OPS-18. The contractor shall provide a Verification of Backups Report in accordance with CDRL A0016, DI-MGMT 81928, Contractor's Progress and Status Report.

4.9.2 The contractor shall verify data restores every 60 days to assure data availability. Per (Performance Requirement Summary & Service Metrics Table 1 & 2)

4.9.3 The contractor shall restore data from backups as directed. Whenever a backup restore is done, it will be entered into the Enterprise Change Management to properly track server configurations IAW with the AAG Configuration Management SOP.

4.10 Security and Data Protection

4.10.1 The contractor shall maintain antivirus signatures and software to prevent against malicious virus attacks using DOD mandated Army End Point Security Solution (AESS).

4.11 Software Services

4.11.1 The contractor shall maintain current patch and updates that are currently utilized by AAG, this includes a number of Commercial Off the Shelf (COTS) and in-house software packages within the enterprise.

4.11.2 contractor shall maintain skilled and certified personnel, in accordance with the requirements in Attachment D.

4.11.3 The contractor shall ensure all software is up to the latest supported security patch/update level.

4.11.4 The contractor shall maintain an inventory of all software installations, to include licenses.

4.11.5 The contractor shall identify and troubleshoot/debug, repair codes that become faulty after patches are applied or if vulnerabilities are identified.

4.12 IT Asset Management

4.12.1 The contractor shall ensure that changes to any IT asset's disposition are accurately reflected in ECM or other approved ticketing system and Government provided software tracking system throughout the asset's lifecycle.

4.12.2 The contractor shall, in writing, notify the COR one (1) year in advance, of any IT asset EOSL (End of Service Life) threshold, including but not limited to hardware, software, software license, or service/maintenance contract unless there is less than a year remaining on some asset EOSL at time of commencement of this contract.

4.12.3 The contractor shall prepare asset for disposal and shipment by sanitizing and excessing assets in accordance with DISA, AAG, and DOD Defense Reutilization and Marketing Office (DRMO) and Army policy. The contractor shall deliver assets to DRMO in the Government provided vehicle.

4.12.4 The contractor shall provide reports on IT asset inventory (CDRL A0001, DI-MISC-80442, Report of Receipts, Inventory, Adjustments, and Shipments of Government Property), per Attachment A - Deliverables.

4.12.5 The contractor shall comply with DOD 4165.06 (Real Property) and Army standards in AR 740-26 (Physical Inventory Control) for Asset Management

4.12.6 The contractor shall ensure that all active IT assets can be located.

4.12.7 The contractor shall maintain documentation for all Asset Management functions, processes, procedures, and training, and make available to all Asset Management Stakeholders IAW SOP-OPS-003.

4.12.8 The contractor shall maintain AAG's Software Asset Management (NIPR and SIPR), Auto Discovery, and License Management.

4.13 Operations Program/Project Management

4.13.1 The contractor shall provide management services for AAG operations initiatives, upgrades, and change requirements. These services should include schedules (i.e. work, maintenance, milestones, patching, lifecycle replacement, upgrades, and planned outages), monthly reports, and actionable task items, tracking of progress and milestones and reporting of project status.

4.13.2 The contractor shall oversee all operations to include project management and task tracking.

4.13.3 The contractor shall maintain a single information store of project management tracking information.

4.13.4 The contractor shall establish a Network Improvement and Availability Plan (CDRL A0011, DI-MGMT-81928, Contractor's Progress and Status Report) demonstrating structures, processes, schedules, reporting requirements and communication channels to accomplish the following:

- Communicate when and why the technical scope of a project changes.
- Communicate when and why scheduled milestone dates change.
- Accurately report when the major project milestones are to be complete.
- Adjust project schedules as necessary if the Government changes project priorities.
- Maintain current status of project deliverables and communicate as needed to all AAG project stakeholders.
- Produce documentation for all project management functions and methodology.
- Facilitate Systems status meetings as required.

4.14 Operations Service Level Management (SLM)

4.14.1 The contractor shall review all SLAs within the Operations division and across at all levels of the AAG Enterprise for delivery of IT services and contract requirement.

4.14.2 The contractor shall institute an internal Service Level Management program to measure compliance with established SLA's.

4.14.3 The contractor shall report to the COR any issues where the contractor can't meet the SLA goals.

4.14.4 The contractor shall perform a series of operational metric reports included in the Monthly Status Report (CDRL A0005, DI-MGMT-81928, Contractor's Progress and Status Report) to demonstrate SLA performance. This will also include all Service Level Management functions process, procedures and training that will be available to AAG stakeholders.

4.14.5 The contractor shall produce documentation for all Service Level Management functions process, procedures and training that will be available to AAG stakeholders.

4.15 Operations Configuration Management

4.15.1 The contractor shall adopt practices to establish and maintain consistency of configuration and operational performance for all AAG IT systems throughout their operational lifespan.

4.15.2 The contractor shall update ECM or other approved ticketing system, which shall accurately reflect the configuration of the current IT environment.

4.15.3 The contractor shall ensure that any configuration changes have been approved by the ICCB and documented in ECM or other approved ticketing system.

4.15.4 The contractor shall produce documentation for all Configuration Management functions process, procedures, and training that will be available to all Configuration Management stakeholders.

4.15.5 The contractor shall perform a series of operational metric reports, as required DI-MGMT-80227.

4.15.6 The contractor shall ensure all hardware and software devices have a DOD compliant and documented configuration per DISA standards.

4.15.7 The contractor shall ensure all hardware and software is kept in compliance with configuration standards.

4.15.8 The contractor shall endeavor to maintain the same configuration across environments for a given application. The contractor shall provide written justification for intentional deviation across environments for a given application.

4.16 Change Management

4.16.1 The contractor shall ensure/utilize standardized methods and procedures are used handling changes to IT infrastructure and will abide by AAG change governance.

4.16.2 The contractor shall maintain a single information store of Change Management data, one for NIPR and one for SIPR.

4.16.3 The contractor shall ensure/utilize Change Management best practices are followed to minimize the impact of Change-related incidents on service availability.

4.16.4 The contractor shall identify and properly document Change Requests that require Government review and await adjudication before implementing changes.

4.16.5 The contractor shall ensure changes are documented according to Change Management best practices and AAG SOPs.

4.16.6 The contractor shall produce documentation for all Change Management functions - process, procedures, and training that will be available to all Change Management stakeholders.

4.16.7 The contractor shall provide reports on change metrics and trends, as required, per (Attachment A - Deliverables)

4.16.8 The contractor shall notify the Government in advance (at a min 24 hrs.) of all scheduled IT changes which have the potential to affect 25% or more of the AAG user community or external customers.

4.16.9 The contractor shall schedule changes which require service outage of scheduled service maintenance windows around the best times to avoid user or customer service loss. Performance of these changes may need to occur during the weekend. All duties that occur on the weekend shall be approved by the COR in advance.

4.17 Incident Analysis and Problem Management

4.17.1 The contractor shall propose and employ methods to minimize the adverse impact of incidents and problems caused by errors within the IT infrastructure and to prevent recurrence of incidents.

4.17.2 The contractor shall institute a method to document and maintain information about problems and the appropriate workarounds and solutions that are visible to the AAG community.

4.17.3 The contractor shall review/maintain/updated documentation (IRP-IMP) for all Incident/Problem Management functions - process, procedures and training that will be available to all Incident/Problem Management stakeholders.

4.17.4 The contractor shall submit trending and metric reports (DI-MGMT-82246), as required, per (Appendix A –Service Metrics) and (Attachment A - Deliverables).

4.18 Knowledge Management

4.18.1 The contractor shall maintain a single information store of Knowledge Management in one tool that provides:

4.18.2 The ability to restrict access to knowledge for different user communities Knowledge Management tool is accessible by multiple users concurrently. Knowledge management tool is accessible only by authenticated/authorized users. Perform Knowledge Management best practices to manage knowledge throughout the knowledge lifecycle.

4.18.3 The contractor shall provide Operational metric reports (DI-MGMT-80227), as required, per (Appendix A –Service Metrics), and (Attachment A - Deliverables).

4.19 Capacity Management

4.19.1 The Contactor shall employ methods to ensure IT capacity meets current and future business requirements in a cost-effective manner.

4.19.2 The contractor shall minimize performance or capacity related service incidents.

4.19.3 The contractor shall troubleshoot/resolve hardware and software workstation related incidents as required within the (Performance Requirement Summary & Service Metrics Table 1 & 2) timelines per ticket severity and provide an Incident Response Report for issues outside of normal duty hours to be provided in the monthly status report (CDRL A0003, DI-MGMT-80368A, Status Report).

4.19.4 The contractor shall produce workload monitoring data of all production and specified test environments services needed by AAG.

4.19.5 The contractor shall review/maintain/update documentation for all functions - process, procedures, and training.

4.19.6 The contractor shall identify to the Government in the Monthly Changes to the Performance & Quality Management Plan any capacity or performance bottlenecks present and recommend action plans to mitigate them (CDRL A0007, DI-MGMT-81928, Contractor's Progress and Status Report).

4.20 Information Assurance (IA) and Systems Security

4.20.1 The contractor shall work with AAG ISSM and ISSO and meet all DOD, DISA, Army, and AAG Operations Information Assurance and System Security Requirements in all AAG supported enclaves to include cloud domains.

4.20.2 The contractor shall comply with AAG's separation of duties for administrator, server, and network accounts.

4.20.3 The contractor shall implement and maintain technical security mechanisms in all AAG supported enclaves (including cloud), which monitor computer security activities, such as the DOD, DISA and Army mandated Host-Based Security System (HBSS), ACAS, Risk Management Framework (RMF), and Network Intrusion Detection Systems (NIDS).

4.20.4 The contractor shall implement and maintain current and future technical security mechanisms.

4.20.5 The contractor shall provide and maintain anti-virus systems for the enterprise using HBSS.

4.20.6 The contractor shall review and maintain server and desktop security using baseline analysis tools built into the HBSS suite and other industry best practices.

4.20.7 The contractor shall recommend security solutions as they become aware of new security industry standards in the Enterprise Information Technology (IT) Performance

Metrics Report (CDRL A0034, DI-MGMT-82246, Enterprise Information Technology (IT) Performance Metrics Report).

4.20.8 The contractor shall adhere to procedures & guidelines to comply with DOD, DISA, Army, & AAG security policies and ensure that all data leaving AAG systems are documented, secured and encrypted.

4.20.9 The contractor shall facilitate and implement the monitoring devices of the AAG and ensure full range of log analysis using SIEM tools for example Netforensics or ArcSight. All associated tasks relating to keeping the equipment running and up to date with current signatures, including operating system upgrades.

4.21 Systems Security Analysis, Defense and Recovery

4.21.1 The contractor shall maintain enterprise data backup strategy (encrypted as required).

4.21.2 The contractor shall monitor and maintain backup and recovery strategies for AAG servers.

4.21.3 The contractor shall schedule and maintain data tape backups of Production AAG servers and other critical data as directed for restoration in the event of a catastrophic loss of the system and/or data.

4.21.4 The contractor shall deliver the initial version of all lifecycle plans (hardware and software) to the Government no later than (NLT) 90 days after contract award, per CDRL A0012 (DI-MGMT-82035A, Software Resources Data Reporting: Development, Maintenance and Enterprise Resource Planning Development Reports, and Data Dictionary).

4.21.5 The contractor shall provide the Final Procedures/Plans based on the final version of the planning documents NLT 90 days after contract award per CDRL A0013, (DI-MGMT-82035A, Software Resources Data Reporting: Development, Maintenance and Enterprise Resource Planning Development Reports, and Data Dictionary).

4.21.6 The contractor shall develop and deliver a document format listing and providing a summarized detail description of all procedures accomplished during the month (CDRL A0016, DI-MGMT-81928, Contractor’s Progress and Status Report).

4.22 Information Assurance Perimeter Defense

4.22.1 The contractor shall develop a plan and monitor all systems to ensure that no unauthorized access points, including wireless access point, are available in any of AAG supported enclaves

4.22.2 The contractor shall ensure that no unauthorized devices are connected, directly or remotely, to the network, desktops or laptops.

4.22.3 The contractor shall detect and report unauthorized software present on AAG systems.

4.22.4 The contractor shall monitor all systems for unauthorized use in accordance with AAG instructions and include incidences of such use in the Monthly Status Report (CDRL A0005, DI-MGMT-81928, Contractor's Progress and Status Report).

4.22.5 The contractor shall deliver the final version of all Plans to the Government not-to-exceed (NTE) a total of 45 days after contract award. The contractor shall provide final procedures based on the final version of the planning documents NTE 90 days after contract award. The contractor shall develop a single page document format listing and providing a summarized detail description of all procedures accomplished during the month, per Attachment A – Deliverables.

4.22.6 The contractor shall adhere to the AAG Incident Response Policy.

4.22.7 The contractor shall document, respond, and report any disruption to the AAG environment, including any unauthorized intrusion that compromises the security of the AAG systems operations.

4.23 Disaster Recovery Planning and Management (AAG DRP Rev 1.5)

4.23.1 The contractor shall maintain and perform routine testing of functional DRP to ensure the integrity of AAG systems operations. The scope of this subtask is all specified in AAG systems operations procedures and approved by the COR in writing.

4.23.2 The contractor shall develop and review data recovery procedures for all media IAW AAG SOP OPS-018. An annual round table exercise with key AAG managers will be conducted per current AAG DRP Rev 15.

4.23.3 The contractor shall test data recovery procedures for all systems backup quarterly and report results.

4.23.4 The contractor shall operate and maintain strict compliance with all applicable Government computer security and IA security acts/laws, mandates, instructions, directives and regulations. The contractor shall meet the IA/Cyber security intent provided by the following Government agencies but not limited to NIST, DISA, Army, Federal laws and AAG security policies.

4.24 Delivery Data

4.24.1 The contractor shall retain all data until the contractor is directed by the Government in writing to dispose of the data.

4.24.2 The contractor shall submit a Monthly Status Report containing a section titled: "Security." and include at a minimum: Identification of unauthorized devices that were connected, directly or remotely, to the network, desktops or laptops, CDRL A0005 (DI-MGMT-81928, Contractor’s Progress and Status Report).

4.24.3 The contractor shall submit a Monthly Status Report containing a section titled: "Security." and include at a minimum: Identification of unauthorized software present on AAG systems (CDRL A0005, DI- MGMT-81928, Contractor’s Progress and Status Report).

4.24.4 The contractor shall submit a Monthly Status Report containing a section titled: "Security." and include at a minimum: Incidences of unauthorized use, as defined in DOD Regulations and AAG instructions (CDRL A0005, DI- MGMT-81928, Contractor’s Progress and Status Report).

4.24.5 The contractor shall submit a Monthly Status Report containing a section titled: "Security." and include at a minimum: IAVA patching status, as defined in DOD Regulations and AAG instructions (CDRL A0005, DI- MGMT-81928, Contractor’s Progress and Status Report).

4.25 Database Support

4.25.1 The contractor shall provide experienced personnel who are certified on Microsoft SQL 2008 R2, and newer databases as required.

4.25.2 The contractor shall provide experienced personnel who are certified on Oracle 11G R2 and newer databases is required.

4.26 Service Availability Monitoring

4.26.1 The contractor shall perform all configuration and maintenance-level database administrative functions.

4.26.2 The contractor shall perform operations in a manner in which the impact on database availability is minimized and in accordance with established AAG standard operating procedures.

4.27 Database Integration Support

4.27.1 The contractor shall ensure operational availability of all database services is integrated with the least possible amount of downtime. Sensitive databases shall be encrypted.

4.27.2 The contractor shall ensure all Change management procedures are followed and adhered to.

4.27.3 The contractor shall complete Planning and documentation prior to new integration or implementation.

4.27.4 The contractor shall plan, test, and implement initiatives to incorporate new technologies not currently present within the AAG web environment.

4.27.5 The contractor shall develop and present for Government approval implementation plans for continual availability improvements for the database services.

4.28 Database Deliver Data

4.28.1 The contractor shall provide a database support Monthly Status Report DI-MGMT-80227.

4.28.2 The contractor shall submit a Monthly Status Report containing a section detailing database service availability, encryption status, capacity and performance.

4.28.3 The contractor shall submit a report with monthly usage statistics, for databases as recorded by the database servers.

4.28.4 The contractor shall retain all data until the contractor is directed by the COR to dispose of the data.

4.29 Database DBA Administration

4.29.1 The contractor shall install database software for all supported releases on all programs managed by AAG no matter the location of database (11GR2 and future releases), per Attachment E – Hardware & Software Listing.

4.29.2 The contractor shall apply Oracle Security Patches per AAG SOP-OPS-09.

4.29.3 The contractor shall create new most current approved version of Oracle databases software.

4.29.4 The contractor shall upgrade all AAG managed Oracle databases to new releases no matter the location of the server.

4.29.5 The contractor shall ensure DBA Support during server migrations, including new installation, and setup on all new servers.

4.29.6 The contractor shall ensure Database Backup Setup and periodic backup verification.

4.29.7 The contractor shall design, test and implement new Database technologies.

4.29.8 The contractor shall provide general user support on database area including LINUX and Windows 2022 and higher issues related to databases.

4.29.9 The contractor shall provide 24 hour-seven day-yearly on-call support for all Oracle, LINUX and Microsoft SQL Server availability.

4.29.10 Cloud Migration and Support (ref 1.1) additional details for cloud support

4.29.11 Provide expertise in supporting and assisting transfer of applications to cloud platforms

4.29.12 The contractor shall assist with customer on-boarding

4.29.13 The vendor shall manage support cloud DevOps and related services

4.29.14 The contractor shall oversee patching in cloud environments

4.29.15 The contractor shall maintain the same level of response cloud environments as the same as AAG on premises production as identified in Table 1 and Table 2 (additional cloud support ticket)

4.30 Systems Support

4.30.1 Uninterrupted Power Supply.

4.30.2 The contractor shall inventory, maintain, deploy, retrieve, and upgrade UPS as needed.

4.30.3 The contractor shall troubleshoot/resolve any associated issues/degraded performance with UPS.

4.30.2 Heating, Ventilation and Air Conditioning (HVAC)

4.30.2.1 The contractor shall maintain temperature within the server room at the optimal per equipment standards.

4.30.2.2 The contractor shall maintain a current humidity/temperature charts in the data center/server room.

4.30.2.3 The contractor shall inventory, maintain, deploy, retrieve, and upgraded HVAC system.

4.30.2.4 The contractor shall troubleshoot/resolve and associated issues/degraded performance with HVAC system

4.31 Unclassified and Classified Marking

4.31.1 The contractor shall prepare for shipment unclassified data in accordance with specified requirements.

4.31.2 The contractor shall prepare for shipment classified reports, data, and documentation in accordance with requirements, or if none is specified, pursuant to the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M and CNSS 1253.

4.32 Protection of Personally Identifiable Information (PII)

4.32.1 To the extent that the work under this PWS requires the contractor to have access to personally identifiable information about an individual (hereinafter referred to as “PII”), the contractor shall after receipt thereof, treat such PII as Controlled Unclassified Information and safeguard such information from unauthorized use and disclosure. The contractor must not appropriate such PII for its own use or to disclose such information to third parties unless specifically authorized by the Government, in writing.

4.32.2 The contractor shall allow access only to those employees who need the PII to perform services under this PWS and agrees that PII shall be used solely for the purpose of performing services under this PWS. The contractor shall ensure that its employees will not discuss, divulge or disclose any such PII to any person or entity except those persons within the contractor’s organization (who have a need to know) directly concerned with the performance of the PWS.

4.32.3 Contractor shall administer a monitoring process to ensure compliance with DOD Privacy Programs. Any discrepancies or issues should be discussed immediately with the COR and corrective actions will be implemented immediately.

4.32.4 The contractor shall report immediately to the AAG Director, Deputy Director, or Security Manager / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual’s first name or first initial and last name in

combination with any one or more of the following data elements including, but not limited to: social security number, EDIP; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

4.32.5 The Government may terminate this PWS for default if the contractor or an employee of the contractor fails to comply with the Privacy Act of 1974 Section (m) (1). Contractors supporting a Government agency shall be considered to be an employee of that agency. All Contractors are required to take Privacy training yearly, provided by the Government, upon hiring and annually. The Government may also exercise any other rights and remedies provided by law or this PWS, including criminal and civil penalties.

4.32.6 In accordance with the Privacy Act or other applicable regulations, additional specialized training may be required per Attachment C – HIPAA Training.

4.33 Applicable Privacy Documents:

4.33.1 DOD Directive 5400.11, January 29, 2019. Subject: DOD Privacy Program.

4.33.2 DOD Regulation 5400.11-R, January 29, 2019. Subject: Department of Defense Privacy Program.

4.34 Health Insurance Portability and Accountability Act (HIPAA)

4.34.1 In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003, the contractor meets the definition of Business Associate. Therefore, a Business Associate Agreement is required to comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and in DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

4.34.2 Definitions. As used in this clause generally refer to the Code of Federal Regulations (CFR) definition unless a more specific provision exists in DoD 6025.18-R or DoD 8580.02-R.in.

4.34.2.1 Individual has the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

4.34.2.2 Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

4.34.2.3 Protected Health Information has the same meaning as the term “protected health information” in 45 CFR 160.103, limited to the information created or received by the contractor from or on behalf of the Government pursuant to the Contract.

4.34.2.4 Electronic Protected Health Information has the same meaning as the term “electronic protected health information” in 45 CFR 160.103.

4.34.2.5 Required by Law has the same meaning as the term “required by law” in 45 CFR 164.103.

4.34.2.6 Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

4.34.2.7 Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160, 162 and part 164, subpart C.

4.34.2.8 Terms used, but not otherwise defined, in this Clause shall have the same meaning as those terms in 45 CFR 160.103, 160.502, 164.103, 164.304, and 164.501.

4.34.3 The contractor shall not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law.

4.34.4 The contractor shall use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

4.34.5 The contractor shall use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Contract.

4.34.6 The contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the contractor of a use or disclosure of Protected Health 4.38.12 4.38.13 Information by the contractor in violation of the requirements of this Clause. These mitigation actions will include as a minimum those listed in the TMA Breach Notification Standard Operating Procedure (SOP), which is available at: http://www.tricare.mil/tmaprivacy/breach.cfm

4.34.7 The contractor shall report to the COR any security incident involving protected health information of which it becomes aware DI-MGMT-80227.

4.34.8 The contractor shall report to the COR any use or disclosure of the Protected Health Information not provided for by this Contract of which the contractor becomes aware.

4.34.9 The contractor shall ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the

contractor, on behalf of the Government, agrees to the same restrictions and conditions that apply through this Contract to the contractor with respect to such information.

4.34.10 The contractor shall ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

4.34.11 The contractor shall provide access, at the request of the Government, and in the time and manner reasonably designated by the Government to Protected Health Information in a Designated Record Set, to the Government or as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524.

4.34.13 The contractor shall make any amendment(s) to Protected Health Information.

4.34.14 Information in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government, and in the time and manner reasonably designated by the Government.

4.34.15 The contractor shall make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the contractor, on behalf of the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner reasonably designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule.

4.34.16 The contractor shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

4.34.17 The contractor shall provide to the COR, in time and manner reasonably designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

4.34.18 The contractor shall review and comply with AAG Special Training per (Attachment C – HIPAA Training).

5.0 General Use and Disclosure Provisions: Except as otherwise limited in this section, the contractor may use or disclose Protected Health Information on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of Protected Health Information would not violate the HIPAA Privacy

Rule, the HIPAA Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government.

5.1 Specific Use and Disclosure Provisions

5.1.1 Except as otherwise limited in this section, the contractor may use Protected Health Information for the proper management and administration of the contractor or to carry out the legal responsibilities of the contractor.

5.1.2 Except as otherwise limited in this section, the contractor may disclose Protected Health Information for the proper management and administration of the contractor, provided that disclosures are required by law, or the contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

5.1.3 Except as otherwise limited in this section, the contractor may use Protected Health Information to provide Data Aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

5.1.4 contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

5.2 Obligations of the Government

5.2.1 Provisions for the Government to Inform the contractor of Privacy Practices and Restrictions. The Government will provide the contractor with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520.

5.2.2 The Government will provide the contractor with any changes in, or revocation of, permission by Individual to use or disclose Protected Health broken in half

5.2.3 Information, if such changes affect the contractors permitted or required uses and disclosures.

5.2.4 The Government will notify the contractor of any restriction to the use or disclosure of Protected Health Information that the Government has agreed to in accordance with 45 CFR 164.522.

5.3 Permissible Requests by the Government

The Government will not request the Protected Health Information in any manner that would not be permissible under the HIPAA Privacy Rule, the HIPAA Security Rule, or any applicable Government regulations (including without limitation, DoD 6025.18-R and DoD 8580.02-R) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the contractor as otherwise permitted.

5.4 Documentation

5.4.1 The contractor shall prepare and maintain adequate documentation (to include server configurations) that allows for the continuous operations of all designated applications, projects and functionality necessary to support the Department of the Army, AAG and their customer base. Additionally, this information shall be stored at an offsite location as well (MIL-STD-2045).

5.4.2 The contractor shall document the processes and procedures utilized to execute all AAG applications and projects in a manner that allows ease of migration from current support vendor to new vendors as approved and validated by the COR (MIL-STD-2045).

5.4.3 The contractor shall ensure current and updated visibility of the status of all critical interfaces with external and/or internal customer base, ensuring visibility at all levels within organization of critical network infrastructure resources and its indicators of health.

5.4.4 Status Reports: The contractor shall submit a Monthly Status Report containing a section titled: “Network Infrastructure Support”. The contractor shall retain all data until directed by the COR to dispose of the data. The Network Infrastructure Support section of the Monthly Status Report (CDRL A0011, DI-MGMT-81928, Contractor’s Progress and Status Report) shall include, at a minimum, the following information:

- Total number of network service outages
- Duration and applications impacted by each outage
- Incident Tracking Activity
- Recommended remediation for outage root cause and any contributing factors, such as procedural anomalies, user error, external effects, etc.
- A report on all cable changes occurring within the month preceding the monthly report
- Reporting on the overall health of the system infrastructure
- Reporting on the End of Life and End of Sale hardware/software and the migration status/plan
- Reports on Network circuit utilization, vulnerabilities and intrusion attempts.
- Financial Expense Reports, to include ODCs, Travel, and Labor.

5.4.5 The contractor shall prepare and maintain a Software Inventory Catalog with adequate documentation that allows for the continuous operation of all designated applications, projects, and functionality necessary to support AAG. (CDRL A0006, DI-MGMT-81756, Software Documentation).

5.4.6 The contractor shall document the processes and procedures utilized to execute all AAG applications and projects in a manner that allows ease of migration from current support vendor to new vendors, as approved and validated with AAG's management and technical staff.

5.4.7 The contractor shall ensure current and updated visibility of the status of all critical interfaces with external and/or internal customer base, ensuring visibility at all levels within organization of critical network infrastructure resources and its indicators of health.

References:

Army Directive 2024-02 Enabling Modern Software Development and Acquisition Practices
DoDI 5000.87 OPERATION OF THE SOFTWARE ACQUISITION PATHWAY

1. Joint Travel Regulations (JTR)
2. Federal Acquisition Regulation (FAR)
3. AAG Change Management Procedures
4. AAG Problem Management Procedures
5. AAG Standard Operation Procedures
6. DOD 8140.30 CYBERSPACE WORKFORCE QUALIFICATION AND. MANAGEMENT PROGRAM
7. http://www.SAM.gov
8. DOD Manual 5200.01 (volumes 1-3) DoD Information Security Program: Protection of Classified Information
9. DOD Manual 5200.02 DoD Personnel Security Program
10. AR 380-67 U.S. Army Personnel Security Program
11. DoD 8140.01 CYBERSPACE WORKFORCE MANAGEMENT
12. DoD 8140.02 IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE. WORKFORCE REQUIREMENTS
13. DoD 8140.03 CYBERSPACE WORKFORCE QUALIFICATION AND. MANAGEMENT PROGRAM
14. AR 25-2 Army Cybersecurity
15. DoD 8500-2 Information Assurance (IA) Implementation
16. DoD 8140 Home Page - DoD Cyber Exchange
17. DODI 8500.01 Cybersecurity
18. AR 525-13 Anti-Terrorism/Force Protection
19. AR 530-1 Operations Security
20. AR 381-12 Threat Awareness and Reporting Program (TARP)