STATEMENT OF WORK (SOW)

For

AUTOMATED INSTALLATION ENTRY (AIE) NEXT

PRODUCTION, TECHNOLOGY INSERTION, AND CAPABILITY SUPPORT

11 January 2023

PREPARED BY:

Product Manager Force Protection Systems

SOLICITATION NUMBER: #W909MY-21-R-G008

PROGRAM: Automated Installation Entry (AIE)

PRODUCT MANAGER: Force Protection Systems (FPS)

PROJECT MANAGER: Terrestrial Sensors (PM TS)

Table of Contents

1.0 SCOPE

This Statement of Work (SOW) defines the effort required for inserting Commercial Off-the-Shelf (COTS) technology upgrades/refresh at previously fielded Army locations and deploying the AIE system to new Army installations. The contractor shall field the AIE system to installations in the continental United States (CONUS) and outside the CONUS (OCONUS). The contractor shall also insert new COTS technology on previously deployed AIE systems in CONUS, Puerto Rico, Alaska, and Hawaii. This effort supports the Capability Support phase of the Defense Business System (DBS), Business Capability Acquisition Cycle (BCAC). It includes the associated program management, technology insertion, Cybersecurity, and logistic support planning requirements.

The selected contractor shall have subject matter expertise and provide all resources necessary to perform the specific requirements as defined in this SOW and individual Delivery Orders (DO). It is not possible for the Government to determine the precise Installation Access Control Point (ACP) requirements, prior to execution of site surveys, for potential locations during the full term of this Indefinite Delivery / Indefinite Quantity (IDIQ) contract. The Government will make every effort to provide the Contractor with ample time to respond to new requirements. However, some DOs may require fast response to address emergent requirements.

1.1 BACKGROUND

Automated Installation Entry (AIE) is the Department of the Army's (DoA) enterprise Installation electronic Physical Access Control System (ePACS) for authenticating personnel against multiple authoritative State and Federal databases. It's an interoperable and integrated solution that supports standardization and automation of Installation Access Control Point (IACP) operations generating efficiencies across the Army Security Enterprise. The AIE system is an Unclassified Information System which optimizes guard force utilization, increases pedestrian and vehicle throughput with enhanced security, allows for adaptation of increased authentication requirements at high threat levels and complies with AR 190-13 for Access Control Standards that includes identity proofing and vetting to determine fitness of an individual requesting and/or requiring access to Installations and issuance of local access credentials.

The System operates within an enterprise network that links AIE sites supporting enterprise operations. The System reads, records and stores credential, biographic and fingerprint information In Accordance With (IAW) Federal Information Processing Standard (FIPS) Publication (PUB) 140-3. The System operates 24 hours a day, 7 days a week. Employment of a remote monitoring capability with access control allows ACPs to be operated during lower Force Protection Condition (FPCON) levels with or without the presence of a guard force.

The AIE Next program has been initiated to design, insert, produce, and deploy an improved AIE system that will fulfill AIE system objectives consistent with the Army Installations of the Future (IoTF) Initiative as described in the AIE Capability Requirements Document (CRD) (Part 2) and AIE Next System Performance Specification (P-Spec), Version 1. AIE Next will improve the Army's enterprise installation electronic physical access control system (ePACS) capability.

The AIE Next P-Spec was developed over the past two years following successful testing and integration of technological improvements to AIE-2 and AIE-3 configurations.

1.2 AIE Installation Access Control Point (ACP) Configurations

1.2.1 Tier-1

Tier 1 ACPs consist of incoming lanes with fixed components that enable traffic flow with minimal supervision. The system has the capability to function with different configurations: Automatic Registration; Gate Arm down; Gate Arm up with traffic light functioning; and Credential Reader. A hard mounted pedestal, located at each lane, contains an intercom, contactless credential reader, 1D and 2D barcode scanner, and front/rear and driver camera to capture the driver's image within a height range of three (3) to seven (7) feet from the ground. Cameras located at the front and rear of the lanes record activity in real-time, including images of license plates. The intercom provides two-way audio communication between the vehicle lane, Guard Booth, Gate House or the Central Remote Station. The user, or ACP Security Officer, scans the driver's credential at the pedestal and the camera records a live image of the driver's face.

1.2.2 Tier-2

The ACPs of some installations manage incoming traffic with wireless handheld lane operations only. Tier-2 lanes operate with wireless handheld credential scanners, provided at each vehicle lane Guard Booth, including a docking station and associated batteries. Tier-2 ACPs shall consist of 1.5 handhelds per lane.

1.3 AIE System Configurations

The AIE-3 Production and Deployment contract began in 2016. Throughout the life of the contract, as new capability was inserted, the AIE-3 system configuration evolved into the current version 4 (AIE-3.4) baseline. Under AIE Next, this configuration baseline will be referred to as AIE-4. At AIE Next contract award, the Government will execute the first Delivery Order (DO) requiring the Contractor to install the AIE-4 baseline configuration in the Government-owned AIE System Laboratory at Aberdeen Proving Ground (APG), MD, in accordance with section 3.2.3.

- AIE-1: 2008, deployed to three (3) locations. Proof of concept capability designated as a closed restricted network (no external communications).
- AIE-2: 2010-2014, deployed to 19 locations. Incorporated lessons learned from AIE-1 to provide an enterprise integrated COTS capability with external communication for automating authentication of registered users.
- AIE-3: Improved on the capabilities provided under AIE-2 to provide the ability for automated registration at the vehicle lane, use of driver's license as a credential, allow one guard to operate two vehicle lanes, and vehicle lane platooning.
    - The current AIE-3.4 baseline configuration provides Cloud operations, enhanced Kiosk capability, enhanced online registration, and In-Lane registration of Driver's License capabilities.

2.0 APPLICABLE DOCUMENTS

The following documents are applicable to this SOW and attached appendices to the extent specified herein.

2.1 Department of Defense (DoD) Specifications

2.1.1 AIE Next System Performance Specification (P-Spec)

2.1.2 AIE Next Concept of Operations (CONOPS)

2.2 DoD Standards, Directives, Instructions, Etc.

2.2.1 DoD Directive 8500.01, Cybersecurity, October 7, 2019

2.2.2 DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, Incorporating Change 1, 11 Aug 2017

2.2.3 DoD Instruction O-8530.2, Support to Computer Network Defense, March 9, 2001

2.2.4 DoD Directive 8500.01, Cybersecurity, March 14, 2014, Incorporating Change 1, October 7, 2019

2.2.5 DoD Instruction 5400.11, Privacy and Civil Liberties Programs, December 8, 2020

2.2.6 Army Regulation 25-1, Army Information Technology, July 15, 2019

2.2.7 Army Regulation 25-2, Army Cybersecurity and associated Department of the Army Pamphlets, April 4, 2019

- Army Pamphlet 25-2-1, Army Cross Domain Solution and Data Transfer Management, April 12, 2019
- Army Pamphlet 25-2-2, Cybersecurity Tools Unified Capabilities Approved Products List Process, April 8, 2019
- Army Pamphlet 25-2-3, Reuse of Army Computer Hard Disk Drives, April 8, 2019
- Army Pamphlet 25-2-6, Cybersecurity Training and Certification Program, April 8, 2019
- Army Pamphlet 25-2-7, Army Information System Privileged Access, April 8, 2019
- Army Pamphlet 25-2-8, Cybersecurity: Sanitization of Media, April 10, 2019
- Army Pamphlet 25-2-9, Wireless Security Standards, April 8, 2019
- Army Pamphlet 25-2-11, Cybersecurity Strategy for Programs of Record, April 15, 2019
- Army Pamphlet 25-2-12, Authorizing Official, April 8, 2019
- Army Pamphlet 25-2-13, Army Identity, Credential, and Access Management and Public Key Infrastructure Implementing Instructions, April 8, 2019
- Army Pamphlet 25-2-14, Risk Management Framework for Army Information Technology, April 8, 2019
- Army Pamphlet 25-2-16, Communications Security (COMSEC), April 8, 2019
- Army Pamphlet 25-2-17, Incident Reporting, April 8, 2019

- Army Pamphlet 25-2-18, Foreign Personnel Access to Information Systems, April 8, 2019

2.2.8 Army Regulation 190-13, Army Physical Security Program, June 27, 2019

2.2.9 MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects & Criticality Analysis, November 24, 1980

2.2.10 MIL-HDBK-217F, Military Handbook: Reliability Prediction of Electronic Equipment, December 2, 1991

2.2.11 Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 22, 2019

2.2.12 NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, April 23, 2021

2.2.13 Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems, March 27, 2014

2.2.14 NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 11, 2014

2.2.15 DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), March 12, 2014, Incorporating Change 3, December 29, 2020

2.2.16 NIST Special Publication 800-63, Digital Identity Guidelines, June 2017

2.2.17 DoDI 5525.19, DoD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB), May 4, 2016

2.3 Non-Government standards and other publications

2.4 Government Furnished Information (GFI)

2.4.1 Identity Matching Engine for Security and Analysis (IMESA) Interface Control Document (ICD) 1.3v10

2.4.2 AIE-4 Hardware and Software List

2.4.3 AIE-4 Operational View (OV-1)

2.4.4 AIE-4 System View (SV-1)

2.4.5 Program Manager Force Protection Systems (PM FPS) Configuration Management Plan (CMP)

2.4.6 AIE-4 System Description and Architecture

3.0 REQUIREMENTS

3.1 General

The Contractor shall field the AIE system to new installations and insert new COTS capabilities that meet the requirements described in the AIE Next P-Spec and supports the AIE Next CONOPS. The integrated System provides the capability to register personnel, authenticate registered users and their credentials and allow authorized personnel access to the Installation.

The System shall be reliable, modular, scalable, open architecture for system and subsystem design supporting lifecycle supportability and capability growth. AIE Next technological solutions shall be based on integrated system performance, industry best practices, long-term availability and supportability. The System shall support future upgrades and integration with other authoritative identity and credential validation sources, biometric systems and other systems to support enterprise capabilities. The System shall provide an interface with IMESA Interoperability Layer Services (IoLS) middleware, IAW DoDI 5525.19 “DoD IMESA Access to CJI and TSDB”, for connection to Defense Enrollment Eligibility Reporting System (DEERS), National Criminal Information Center (NCIC) and to the Federal Bridge for additional sources to vet user data through each Installation’s Site Server. The System shall perform vetting of visitors independent of IoLS via the Installation’s Originating Agency Identifier (ORI) connection to the NCIC (Interstate Identification Index (III) files), DMV and in-state or out-of-state law enforcement sources.

The Contractor shall utilize and build upon the existing baseline hardware and software to maintain and build upon existing capabilities. The primary overarching objectives are:

- Maintain/Increase a high level of initial and continuous security vetting
- Improve ease of access while maintaining security
- Return on Investment.

3.2 Detailed Tasks

3.2.1 Enterprise Capabilities

The AIE System interfaces directly with the enterprise servers (primary and secondary) and maintains the existing capabilities. The site servers connect to IoLS for access to DEERS, the local database, NCIC and out to the Federal Bridge. The Contractor shall ensure that ongoing Enterprise operations are maintained throughout execution of each Installation DO with minimal system disruption.

3.2.2 Cybersecurity

The Contractor shall establish a Cybersecurity program to implement and sustain Cybersecurity management, administrative, operational and technical controls and processes required to safeguard DoD information systems from unauthorized access and disclosure. Protection measures applied must prove commensurate with the risks of loss of data, misuse, unauthorized access or modification of information.

The Contractor shall ensure the AIE System obtains/maintains a DoD system accreditation and connection approval to an Installation’s NIPRNET IAW DoD Directive (DoDD) 8500.01,

Cybersecurity, and DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), AR-2 to include applicable sub publications and other new Policy, Directive, Operational Orders, Cybersecurity Task Order and Publications. The contractor shall complete risk validation testing before RMF package is submitted for ATO approvals. The AIE System is categorized as Moderate, Moderate, Moderate for Confidentiality, Integrity, Availability (CIA) with an overall impact level of Moderate and operates on the Army LandWarNet NIPRNET environment. AIE system is consent authorized to initial and unannounced vulnerability assessments by federal authorities. The Contractor shall account for and address all DoD Security Controls assigned in the RMF package at the Moderate, Moderate, Moderate Level for the AIE system. The Contractor shall develop, track and implement assigned Security controls including inherited Security controls via System Implementation Plan and IT Security Plan of Action and Milestones (POA&M). The accreditation documentation shall be developed and delivered IAW CDRL A002 Information Systems Accreditation Documentation and CDRL A003 monthly Vulnerability Scan Compliance Report. The plans include but not limited to the Security control implementation status, security control designation, responsible entities, resources, the estimated completion date for each assigned Security control and System-level Continuous Monitoring (SLCM) Strategy

3.2.2.1 Risk Management Framework (RMF). The Contractor shall be familiar with the DoD RMF for DoD IT policy guidance. The Contractor shall input all required artifacts and populate all required fields in the eMASS package in support of the RMF process and package submission for ATO. The cybersecurity requirements for DoD IT shall be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. All DoD Information Systems must be categorized IAW Committee on National Security Systems Instruction (CNSSI) 1253 and implement a corresponding set of security controls from NIST SP 800-53 Revision 4. The assessment procedures from NIST SP 800-53 Rev 4 and DoD-specific assignment values, overlays, implementation guidance and assessment procedures shall be used. The Contractor shall implement and complete the comprehensive self-assessment with supporting documentation upon receiving the Army's RMF policy guidance for operational testing approvals, Interim Authority to Test (IATT) and ATO approvals.

3.2.2.2 Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs). The Contractor shall ensure AIE system configuration continues to be IAW applicable DISA STIGs. STIGs are product-specific and document applicable DoD policies, security requirements, best practices and configuration guidelines. STIGs are associated with security controls through Control Correlation Identifiers (CCIs) which are decompositions of NIST SP 800-53 Rev 4 security controls into single, actionable and measurable items. Security Requirements Guides (SRGs) are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, a SRG may be used. STIGs, SRGs and CCIs are available on the DoD Cyber Exchange at https://public.cyber.mil. Updates to STIGs, SRGs, and CCIs shall be executed when DISA releases updates or upon system change.

To ensure continued adherence to applicable DISA STIGs, the Contractor shall:

- implement a network device management solution; and
- implement a Mobile Device Manager (MDM) solution that will control and configure the wireless handheld scanners; and

- implement Assured Compliance Assessment Solution (ACAS) in accordance with Army and DoD directives; and
- conduct monthly scans to include all devices within the AIE network, STIG Viewer checks, apply applicable checklists, implement vendor security guidance, utilize industry best practices and any applicable vendor product security patches periodically to remediate/mitigate system vulnerabilities; and
- document and provide remediation/mitigation efforts of ACAS scans and STIG findings to the Cybersecurity Representative; and
- update/upgrade ACAS and STIG Viewer to newer versions within 20 days of release by DISA, to ensure vulnerabilities are identified as soon as possible; and
- leverage DISA approved vulnerability remediation tools and latest plug-ins or weaknesses mitigation in the application design/coding phase, such as those described in the Common Weakness Enumeration/System Administration, Networking and Security Institute (CWE/SANS) TOP 25 Most Dangerous Programming Errors, and Open Web Application Security Project (OWASP) Top Ten; and
- provide all required information IAW CDRL A003.

The Contractor shall use DoD approved vulnerability assessment tools to test and validate the overall security posture of the AIE system. The Contractor shall document STIG and SRG compliance results, for products, as security control assessment results within a product-level Security Assessment Report (SAR). The SAR shall be submitted for review to the responsible Government Information System Security Manager (ISSM) and Security Control Assessor (SCA) (formerly the Agent for the Certification Authority (ACA)) for acceptance or connection into an authorized computing environment. This review ensures products will not introduce vulnerabilities into the hosting DoD Information System.

The SCA's risk assessment will be used by the SCA to determine the level of overall system cybersecurity risk and a basis for recommendation for risk acceptance or denial to the Authorizing Official (AO) (formerly the Designated Accrediting Authority (DAA)). The SCA's risk assessment considers threats, vulnerabilities and potential impacts as well as existing and planned risk mitigation. The risk assessment will address all Non-Compliant (NC) controls and clearly communicate the SCA's conclusion on system cybersecurity risk and any recommendations for special instructions to accompany the authorization decision. Actual results of the SCA's risk assessment are recorded in the SAR and POA&M as part of the security authorization package, along with any artifacts produced during the assessment (output from automated test tools or screen shots that depict aspects of system configuration).

The Contractor shall apply applicable DISA STIGs, checklists, vendor security guidance, industry best practices and applicable vendor product security patches. The contractor shall ensure applications are in compliance with DoD Instruction 8500.2 Cybersecurity Implementation (current version) and DoDI 8551.1 Ports, Protocols and Services Management (PPSM).

3.2.2.3 Information System Enclave Accreditation Security Posture. The Contractor shall continuously maintain, review and assess the status of the System as it relates to Information System Enclave accreditation security posture. The Contractor shall adhere to Security controls that relate to configuration and vulnerability management, performance monitoring and implement capabilities to continuously monitor the System and information

environment for security-relevant events and configuration changes that negatively affect security posture. The system-level continuous monitoring strategy must conform to all applicable published DoD enterprise-level or Army continuous monitoring strategies. The Contractor shall report significant changes in the security posture of the System IAW CDRL A003 and immediately recommend mitigation strategies to the Government. At the direction of the SCA or AO, the Government may schedule a revalidation of any or all Security controls at any time.

3.2.2.4 Authority To Operate (ATO). When required, the contractor shall prepare and have the connection approval ready in support of operational testing (IATT). The Contractor's COTS technology insertions shall be capable of obtaining, supporting and maintaining the AIE system's ATO accreditation decision to connect to the Army's LandWarNet which is based on achieving an ATO and maintaining an acceptable risk posture. The AIE system is characterized as a "type authorization" which is used to deploy identical copies of a DoD Information System in specified environments. This method allows a single security authorization package and baseline to be developed for a Type Accredited as Information System Enclave.

The Contractor shall execute corrective actions to resolve all security weaknesses identified during the Assess & Authorize process associated with the design, engineering, integration, configuration, implementation and documentation of the AIE solution which will be recorded and tracked in a System Security POA&M. The Contractor shall prepare the POA&M, IAW CDRL A002, based on the vulnerabilities identified during the security control assessment. Inherited vulnerabilities must be addressed on the POA&Ms. POA&Ms shall be updated throughout a System's life cycle as vulnerabilities remain, are remediated, or new vulnerabilities are discovered. All non-compliant (NC) and non-applicable (NA) security controls must be documented in a POA&M with an explanation of remediation actions. If a risk needs to be submitted for risk acceptance, justification as to why accepting the risk of operating the System with NC control status shall be submitted.

3.2.2.5 System Security Plan (SSP). The Contractor shall develop an AIE SSP IAW CDRL A002 that provides an overview of the security requirements for the System and describes the security controls in place or planned for meeting those requirements. The Contractor shall input required data in the Enterprise Mission Assurance Support Service (eMASS) package which allows for the output of a Security Plan Report in eMASS. The security plan shall include implementation status, responsible entities, resources and estimated completion dates. Security plan shall include a compiled list of system characteristics or qualities required for system registration and key security-related AIE documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan and incident response plan. The Government approves the SSP prior to implementation which establishes the level of effort required to successfully complete the remainder of the steps in the RMF and provides the basis of the security specification for the acquisition of the system, subsystems or components. The AO's approval of the security plan must be documented in the security plan.

The ISSP shall include the Contractor's strategy for implementation of Cybersecurity requirements throughout the life of the contract. The security plan shall address the security controls described in NIST SP 800-53 and should be tailored in scope and depth appropriate to the effort and the specific unclassified DoD information IAW DoDI 8510.01.

3.2.2.6 Cybersecurity Vulnerability Management (IAVM). The Contractor shall continuously assess and monitor security policies and procedures to incorporate a Cybersecurity Vulnerability Management (IAVM) program as referenced under DoDI O-8530.01, dated 07 March 2016 and Chairman Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), dated 09 June 2015, into the AIE deployment and production environments. The Contractor shall comply with the requirement for IA Vulnerability alerts, bulletins and technical advisories IAW CDRL A003, Vulnerability Scan Compliance Report. The Contractor shall test all patches, upgrades and new applications prior to monthly and/or after emergency deployment. The Contractor shall continuously monitor, maintain, review and assess the status of the System as it relates to the accreditation and system security posture. The Contractor shall assess and implement remote patching management via remote means to remediate technical vulnerabilities during Cybersecurity Vulnerability Management process. Depending on the vulnerability, remediation will be combination of the proposed solutions of WSUS, SCCM, Solar Winds, or SOTI and remediation solution shall be provided to PM FPS.

3.2.2.7 Vulnerability Assessments. The Contractor shall conduct vulnerability assessments IAW CDRL A003, Vulnerability Scan Compliance Report, after any configuration engineering changes to the system baseline and emergency patch releases. During the 12-month CLS period, the Contractor shall conduct quarterly vulnerability assessments (using DoD approved products) and install system updates to ensure IA maintenance compliancy with updated security requirements. The Contractor shall ensure a final vulnerability assessment and full system update is complete prior to transitioning to an installed system for Government sustainment operations.

3.2.2.8 Privacy Impact Assessment (PIA). The Contractor shall ensure the AIE System continues to protect Personally Identifiable Information (PII) IAW the Privacy Act of 1974, DoD Privacy Program, implemented by Department of Defense Directive (DoDD) 5400.11, DoD 5400.11-R and applicable Federal laws regarding the protection of privacy information. The System shall comply with the DoD Personnel Identity Protection (PIP) program as implemented by DoD 1000.25. To ensure privacy protections are maintained, the Contractor shall conduct PIAs IAW CDRL A004.

3.2.2.9 Information System Security Engineering (ISSE). The Contractor shall provide system-level support IAW references cited in the P-Spec and provisions of DoDI 8510.01, DoDI 8500.2, Army Regulation 25-1, Army Knowledge Management and Information Technology and Army Regulation 25-2, Army Cybersecurity. The Contractor shall engineer and implement all DoD technical and security control requirements that facilitates the operational capabilities of the system.

3.2.2.9.1 Endpoint Security (ENS) / Host Based Security System (HBSS). The Contractor shall use the DoD-provided, enterprise-wide automated HBSS solution for the remediation of vulnerabilities. The Contractor shall implement, maintain, and update modules as mandated by Army and DoD policy. The HBSS agent with the current mandated modules will be installed on all windows machines as part of the delivery order baseline build. HBSS shall include applicable modules (example: ENS, HIPS, EDS, EPP DOP, PA, RSD and ACCM add onto HBSS agent with anti-virus). The Contractor shall implement and maintain new and updated HBSS modules as they are released, deploy and configure HBSS to all servers and

workstations, continuously monitor ENS/HBSS for system anomalies, and address performance issues with HBSS as they may arise.

The system is required to perform an end-to-end automated deployment of patches and updates to IT devices using enterprise patch management tools to include configuring access to the DoD Windows Server Update Services (WSUS) located on the DoD Patch Repository website. The Contractor shall deploy critical Microsoft patches within one week of notification publication by Microsoft and implement Microsoft System Center Configuration Manager (SCCM) to support deployment of updates that are not supported in WSUS. Third party patches and software updates shall be coordinated by the Contractor and applied within 30 days of version release or update. The Contractor shall engineer and implement an automated, continuous on-line monitoring and audit trail creation capability with the ability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications. The capability shall be user configurable to automatically disable the system if serious IA or software violations are detected. The system shall employ an automated tool to review audit log records and reports. The system shall be designed with a hierarchical organizational unit (OU) structure that is adaptable and sustainable.

3.2.2.9.2 Enterprise SPLUNK / Solar Winds. The Contractor shall implement an Enterprise SPLUNK / Solar Winds capability to support continuous monitoring of all Windows and network devices. The following data types shall be collected and provided to Product Manager Force Protection Systems via Splunk:

- Active Directory Logs
- Agent Log
- Application
- Central Processing Unit
- Cisco ASA (Firewall) (Beta)
- Computer
- Daily Performance Monitoring
- Disk Space
- Error Log
- Hawkeye
- Hawkeye Daily Performance Metrics (Beta)
- Hawkeye Versions By Host
- IIS Logs
- Network Device Logs
- Operational Logs (Only specific Lines)
- Performance Counters
- Performance Metrics (Beta)
- Processes
- Processor
- RAM
- Routers/Switches/WAPs etc. (TBD)
- Security
- Setup
- SQL Server

- System
- Windows Event Logs
- Windows Host Monitoring
- Windows Installed Applications
- Windows Listening Ports
- Windows Performance Monitoring
- Windows Update logs

3.2.2.9.3 Security Test and Evaluations (ST&E). The Contractor shall conduct ST&Es, as required upon application of security patches, to accurately assess the system's security posture. The ST&Es will be conducted to uncover design, implementation and operational flaws that may affect the confidentiality, integrity and availability of the AIE System. The Contractor shall provide ST&E results, along with the RMF Body of Evidence (BOE), via the Enterprise Mission Assurance Support Service (EMASS). The Contractor, as required, shall support the Federal Information Security Management Act (FISMA) yearly assessments. The Contractor shall provide documents, data, certification test results and access as required for major changes and recertification. The Contractor shall maintain the AIE Security and Impact Analysis (SIA) to show all of the system add-ons and changes within the system.

3.2.3 AIE System Government Laboratory

The Contractor shall install the AIE-4 baseline configuration in the Government Laboratory and be prepared to conduct a system Functional Configuration Audit IAW section 3.2.3.1, Production Qualification Test (PQT) IAW section 3.2.6.7.2, Logistics Demonstration (LD) IAW section 3.2.7.1.3, and Physical Configuration Audit (PCA) IAW section 3.2.4.4.3.2, within 90 days after initial DO award. Upon Government acceptance, the AIE System Laboratory will be used to support DoD certification and accreditation, life-cycle IA measures, testing system modifications, software updates and facilitate Government helpdesk support and troubleshooting. The lab system shall interface with the IoLS test environment to support test and acceptance. The Contractor shall utilize the AIE System Laboratory for final verification of software and hardware changes and present change request to the Configuration Control Board (CCB) for approval.

The Contractor shall provide an operational system based on the approved baseline design including all hardware, software and network equipment. The System shall include Site Servers, Registration Station and equipment for one ACP and two lanes. The System shall be capable of being expanded with equipment for additional lanes and registration stations. The Contractor shall provide a recommended equipment layout in the laboratory and installation/setup instructions to include integration with the existing enterprise servers.

The Contractor shall prepare a Failure Modes and Effects Criticality Analysis (FMECA) Report IAW CDRL A005. The FMECA shall be consistent with the proposed design and IAW Military Handbook (MIL-HDBK)-217F - Reliability Prediction of Electronic Equipment; Military Standard (MIL-STD)-1629A - Procedures for Performing and Failure Mode, Effects and Criticality Analysis; and MIL-HDBK-472 - Maintainability Prediction and Non-electronics Parts Reliability Data (NPRD)-95. The documentation provided shall contain detailed information to allow for Government evaluation of Mean Time Between Failure (MTBF), Mean Time Between Critical Failure (MTBCF) and

Operational Availability (Ao). The FMECA shall be traceable to the submitted system design and demonstrate clearly how the Contractor arrived at its values for system MTBF, MTBCF and Ao.

3.2.3.1 Functional Configuration Audit (FCA). The Contractor shall conduct a FCA, witnessed by the Government, for each system Configuration item (CI). The FCA shall verify the CI meets requirements stated in the System Performance Specification (SPS) and ensure requirements traceability. The Contractor shall provide a FCA Plan IAW CDRL A041 and FCA Report IAW CDRL A042.

3.2.4 Systems and Technology Deployment

3.2.4.1 New Sites. "New Sites" is defined as DoD facilities with no existing AIE equipment. The Contractor shall field the AIE Next system to (up to 62) new sites in the Continental United States (CONUS) and (up to 30) new sites Outside the Continental United States (OCONUS). Potential OCONUS new sites are located in Europe (USAEUR) and the Pacific (USARPAC). It is anticipated that the Tier-2 configuration will be installed at all 92 new sites. Specific location of each new site will be provided following base contract award. For source selection purposes, the Pricing Model provides estimated site quantities (by size) per year as well as size descriptions (number of ACPs and lanes).

3.2.4.2 COTS Technology Insertions. The Contractor shall develop a technology insertion program that supports verification of subsystems and/or components, when integrated with AIE, that meet requirements described in this SOW and the AIE Next P-Spec. The insertion program shall include planning, execution, and assessment of capability performance against the AIE Next P-Spec. The Contractor shall design, integrate, test, and evaluate new functional capability with mature hardware and software technologies necessary to satisfy program requirements for performance, logistics support, and operation of the AIE system. The Contractor shall outline site deployment methodology and provide a deployment schedule IAW CDRLs A015 and A016 (see section 3.2.4.2 and 3.2.5.2) for each technology insertion DO. New technology insertions shall be executed IAW section 3.2.6.4 "Engineering Change Proposals."

The Contractor may require incidental Commercial off-the-shelf (COTS) Hardware and Software to hardware software integration. If related incidental hardware and software are required for a particular task, the Contractor shall purchase these items, if available, under the CHESS hardware contracts or Enterprise Software License providers as they are the preferred source of supply. For Army users, it is the mandatory source for hardware and software IAW Army Federal Acquisition Regulation Supplement (AFARS) 5139.101. The CHESS website at https://chess.army.mil provides a representative sample list of Commercial IT Products and Services authorized for use by customers worldwide. A request for quote may be submitted for products not found on the CHESS site. If the hardware and related software required is not available from a CHESS contract or the authorized list, the contractor shall be authorized to obtain the hardware through an alternate source. For Army users, a Statement of Non-Availability (SoNA) is required for purchase of products from another source regardless of dollar value. Customers can access the SoNA process at https://chess.army.mil/Content/Page/SONA.

3.2.4.3 Technology Refresh. The Contractor shall upgrade previously deployed AIE systems with the latest version of system components for equipment that is no longer

supportable or unable to meet existing/planned requirements. The refresh rate of many AIE components is 5 - 7 years. See section 3.2.4.4.3 for anticipated number of sites requiring technology refresh during the 6-year PoP.

3.2.4.4 Site Deployment Operations

3.2.4.4.1 Site Survey. Prior to installation the Contractor shall perform a physical site survey and deliver a Site Survey Report (SSR) IAW CDRL A008. The SSR shall include number of ACPs and entry lanes, visitor control center, contractor work area, Network Enterprise Center (NEC)/Directorate of Information Management (DOIM) server locations, Garrison network layout to support system design, space requirements for training and storing spares and equipment, and remediation requirements which are existing site conditions requiring modifications or upgrades to accommodate the AIE System installation. The Contractor shall include an assessment of fiber optic cable availability and network architecture to support system requirements and verify and document the availability of NEC/DOIM communication pathways. The Contractor shall collect all information required to support either the Fixed-Full or Handheld design as applicable in the DO.

3.2.4.4.2 Site Design. The Contractor shall develop a detailed Installation-specific Installation Engineering Plan (IEP) IAW CDRL A009. The design shall be IAW Government-provided Technical Data and any technical enhancements integrated during the life of the contract. The design shall incorporate Installation-specific items including: executive summary, site description, fielding schedule, building and utility system diagrams, BOM, Engineering Drawings, Installation maps, system integration diagrams, construction permitting requirements, and intrusion detection systems. The System design shall include integration of the System with the Installation's network and any existing Installation entry technologies and capabilities. If applicable, the design shall interface with the ACPEP site preparation work completed IAW the Army Access Control Points Standard Design, dated May 2013.

The IEP shall include site remediation requirements which are existing site conditions requiring modifications or upgrades to accommodate the AIE System installation. The remediation requirements shall be identified during site survey and included in the SSR. The Contractor shall submit a remediation proposal upon Government acceptance of the IEP if necessary.

3.2.4.4.2.1 National Law Enforcement Telecommunication System (NLETS). The Contractor shall develop a Criminal Justice Information Services (CJIS) Security Plan IAW CDRL A010 for each site requiring an NLETS connection in order to use the site’s ORI. The plan shall focus on Security Operations Supporting AIE CJIS Interface for CJIS data processing of vetting visitors through NLETS. The Plan shall be developed in accordance with FBI CJIS Security Policy (CJISD-ITS-DOC-08140-5.9) to include solution description, vetting process description, roles and responsibilities, site configuration diagram, and FBI CJIS Security Addendum. The site POC will staff the CJIS Security Plan for state approval. The Contractor shall coordinate with each local NEC, each local Internet Service Provider (ISP) and State/County Law Enforcement to create an interface for development and testing.

3.2.4.4.2.2 Initial Design Review (IDR). The Contractor shall conduct an IDR for each site. The IDR shall be conducted at the gaining Installation or via teleconference at the discretion of the Government and IAW the associated DO. During the review, the Contractor

shall present proposed architecture and equipment models and highlight technical issues requiring Government guidance or resolution.

3.2.4.4.2.3 Final Design Review (FDR). The Contractor shall support a Government-led FDR no later than 10 days following receipt of the final IEP. The FDR shall be conducted at the gaining Installation or via teleconference at the discretion of the Government and IAW the associated DO. The Government has final approval authority of the final design.

3.2.4.4.3 Site Installation. The Contractor shall install a complete and fully functional system or technology insertion as defined in the Government approved, site specific, IEP. The Contractor shall execute all aspects of fielding to include: remediation (as required), site preparation, installation of equipment, integration, interface with existing infrastructure, and on-site user support immediately following Government site acceptance. The Government anticipates fielding the AIE system to 92 new sites and fielding new COTS technology to 50 previously fielded sites.

3.2.4.4.3.1 Operational Testing. The Contractor shall conduct on-site operational testing IAW section 3.2.6.7.3 “Performance Verification Test (PVT): Government Acceptance Testing.” Government site acceptance criteria is described in CDRL A021. Test objectives include determination and execution of corrective actions and subsequent demonstrations necessary to verify requirements met; and validation of system level training.

3.2.4.4.3.2 Physical Configuration Audit (PCA). The Contractor shall conduct a PCA, witnessed by the Government, following completion of required testing. A PCA shall be conducted for each system site installation and technical insertion. Following correction of all failures, the system site configuration shall be baselined. The PCA shall confirm proper execution of the IEP and ensure traceability to the Site Technical Data Package (see SOW section 3.2.4.4.3.3). The Contractor shall provide a PCA Plan IAW CDRL A011 and PCA Report IAW CDRL A012.

3.2.4.4.3.3 Site Technical Data Package (TDP). At completion of the System or Technology Insertion install, the Contractor shall provide a Site TDP IAW CDRL A013 documenting the installed System or new technology, prepared site maps and as-built drawings. The Contractor shall deliver a final Site TDP prior to Government acceptance at each Installation. For technology insertions at previously fielded sites the Contractor shall update Government provided (GFI) site TDPs IAW CDRL A013.

3.2.5 Program Management

The Contractor shall perform program management functions that ensure delivery of an integrated AIE System within the contract cost, schedule and performance parameters. The Contractor shall provide qualified personnel, resources and processes to manage multiple simultaneous DOs that include site survey/design and fielding while supporting the technical evolution of the System. Program management functions shall provide the capability to identify program risks and mitigations; incorporate customer feedback to improve cost, schedule and performance over the POP.

3.2.5.1 Contractor’s Management Plan. The Contractor shall provide a Contractor’s Management Plan IAW CDRL A014. The Contractor’s Management Plan shall include a

Program Management Structure that identifies the education and experience level of the following proposed key personnel: Program Manager, Deputy Program Manager, Contract Manager, Fielding Manager, System Engineering Manager, Quality Assurance Manager, Configuration Manager, Cybersecurity Manager, Test Manager and Logistics Manager. The Contractor shall identify the Management Control System (MCS) to be used to integrate program execution by DO and across the entire contract. The Contractor shall document the processes and procedures used to implement and maintain the MCS. The Contractor's Management Plan shall include quality assurance and risk management with mitigation strategies.

3.2.5.2 Integrated Master Schedule (IMS). The Contractor shall develop an Integrated Master Schedule (IMS) IAW CDRL A015 for each DO that includes all tasks, durations, predecessors and successors required to successfully execute the DO.

3.2.5.3 Bi-Weekly Schedule Report. The Contractor shall provide a Bi-Weekly (every two weeks) Schedule Report IAW CDRL A016. The report shall be structured to provide an up-to-date schedule of contract activities for all active DOs.

3.2.5.4 Integrated Program Review (IPR). The Contractor shall conduct a monthly IPR with the Government. IPRs shall cover status of each awarded DO, CDRL submissions, program risks and mitigations, Cybersecurity, financial status, quality/performance metrics, contractual actions and CLS sustainment status. Government attendees will include the Office of the Provost Marshal (OPMG) AIE Functional Lead, Army Corps of Engineers (ACoE) ACP PM, FPS Installations Project Officer, Contracting Officer, AIE Assistant Program Manager (APM), Contracting Officer's Representative (COR), AIE Program Staff (Fielding Manager, Technical Lead, Systems Acquisition Manager, Site Managers, Budget Analyst, and Cybersecurity Lead), and AIE user representation from the Army Installations.

3.2.5.5 Contractor Manpower Reporting. The Contractor shall report all Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via the SAM.gov secure data collection site. The Contractor is required to completely fill in all required data fields within the SAM.gov using the following web address: SAM.gov/Home 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 2022. Contractors may direct questions to the help desk at: SAM.gov | Help. To fulfill this Army reporting requirement, the following information is provided:

Contracting Officer Representative (COR) Name: (will be added at time of award)
The Unit Identification Code (UIC) for the COR is:
The Federal Service Code (FSC) for the COR is:
The Command Code for the COR is:
Fiscal Funding Station Code:

Additionally, the Contractor shall provide a monthly Contractor's Progress, Status & Management Report IAW CDRL A017. The report shall be structured to provide an up-to-date status of the Contractor's technical, operational, financial and programmatic progress.

3.2.5.6 Data Repository. The Contractor shall use the Government-designated data repository as an Integrated Data Environment (IDE), which provides information sharing among participants to include a comprehensive document repository for all programmatic documents and deliverables.

3.2.5.7 Meetings and Briefings. The Contractor shall participate in meetings to manage all areas of the program to include planning, programming, controlling and execution. These meetings shall include Start-of-Work Meetings, Technical Interchange Meetings, Integrated Product Teams (Bi-Weekly IA, Monthly Supportability) and monthly Program Management Reviews. The Contractor shall be responsible for recording, producing and distributing meeting/briefing minutes and tracking of action items for all meetings and briefings. The Contractor shall create, review and provide technical briefings, graphics support and/or other presentations, as required. Meetings and briefings shall be prepared and recorded IAW CDRL A018. Government attendees may include PM FPS and staff, the Office of the Provost Marshal (OPMG) AIE Functional Lead, Army Corps of Engineers (ACoE) ACP PM, FPS Installations Project Officer, Contracting Officer, AIE Assistant Program Manager (APM), Contracting Officer's Representative (COR), AIE Program Staff (Fielding Manager, Technical Lead, Systems Acquisition Manager, Site Managers, Budget Analyst, and Cybersecurity Lead), and AIE user representation from the Army Installations.

3.2.6 Systems Engineering

The Contractor shall provide qualified systems engineering and technical support to meet the mission. The Contractor shall prepare, submit and maintain a System Engineering Management Plan (SEMP) IAW CDRL A019. The Contractor shall conduct systems engineering analysis as necessary to ensure it meets P-Spec requirements. The SE processes shall support design, fielding, logistics, maintenance, system requirement management and system architecture upgrade according to the Contractor's SEMP.

3.2.6.1 Software Quality Assurance Plan. The Contractor shall develop and implement a Software Quality Assurance Plan IAW CDRL A007 to provide quality assurance of software processes and deliverables. The plan shall describe the Contractor's subsystem and system-level processes used to ensure software products undergo Computer Software Configuration Item (CSCI) level testing and validated in accordance with the systems engineering requirements decomposition. Major events within the Software Quality Assurance Plan shall be reflected in the IMS. Major events include, but are not limited to Software Quality Audits, Software Configuration Audits, and Software Qualification Testing. Software Quality Assurance shall flow to vendors and subcontractors that produce software products used in meeting program requirements.

The contractor shall implement selected software metrics to provide management visibility into the software integration process and progress. The contractor shall apply core software metrics, as a minimum. The selected metrics shall clearly portray variances between actual and planned performance, shall provide early detection or prediction of situations that require management attention, and shall support the assessment of the impact of proposed changes on the program. The contractor shall provide the program office routine insight into these metrics.

The contractor shall include software processes, tasks, reviews, and events in the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS). The contractor shall ensure the IMP, IMS, and Software Development Plan (SDP) include the processes, events, and criteria to manage the technical performance characteristics and associated margins and tolerances of the hardware and software.

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

The Contractor shall establish and maintain a hardware-in-the-loop, software/system integration lab (SIL) for Contractor Verification Testing. The lab shall support software regression, null valve, and out of bound testing. The lab must be within 100 miles of the PMO office.

3.2.6.2 System Description and Architecture. The Contractor shall develop a System Description and Architecture Document IAW Contract Data Requirements List (CDRL) A001 to document the technical solution. The architecture shall support the AIE Operational View (OV-1) and System View (SV-1) (Appendix A).

3.2.6.2.1 Interface Requirements Specification (IRS). The Contractor shall develop an IRS IAW CDRL A043 to document the requirements imposed on the AIE system or components to achieve one or more interfaces.

3.2.6.2.2 Software Design Description (SDD). The Contractor shall develop a SDD IAW CDRL A044 and a Database Design Description (DBDD) IAW CDRL A046 to document the Computer Software Configuration Item (CSCI) design.

3.2.6.2.3 Interface Design Description (IDD). The Contractor shall develop an IDD IAW CDRL A045 to document the interface characteristics of the AIE system.

3.2.6.3 System Update and Implementation Plan. The Contractor shall deliver a System Update and Implementation Plan IAW CDRL A047. The plan shall include a cost/benefit analyses and define all facilitation, training and support requirements and responsibilities to help the Government manage the proposed acquisition in a cost effective and timely manner.

3.2.6.4 Engineering Change Proposals (ECP). As required, the Contractor shall submit Engineering Change Proposals (ECP) IAW CDRL A006. The ECP shall describe the Contractor's approach with recommendations proven at Contractor's expense. The ECP shall include Contractor's actions to ensure viability of the new technology and incorporation within an Information system Enclave concept. Contractor recommendations may include: incorporation of new COTS technology capabilities; integration with other physical security systems, authoritative sources (for validation of identity and credentials); biometric systems; operating system upgrades and Chemical, Biological, Radiological, Nuclear, or High Yield Explosives detection and non-intrusive inspection capabilities. New COTS technology must be

at Technology Readiness Level (TRL) 7 prior to integration. The Government may request and the Contractor may propose system updates.

3.2.6.5 Requirements Traceability Matrix (RTM). The Contractor shall develop, deliver and maintain a RTM IAW CDRL A001.

3.2.6.6 Technology Research and Evaluation (RDT&E). The Contractor shall provide or support research and evaluation of new and emerging technology for potential insertion into the AIE system to satisfy mission requirements based on a business case analysis. These tasks may include but are not limited to, analytical capabilities, infrastructure innovation, data innovation, access control technological advancements, and other strategic innovations. The RDT&E shall comprise of practices that enable rapid fielding of Industry-proven capabilities.

3.2.6.7 Test and Evaluation. The Contractor shall develop a test program that will support verification that the System meets requirements contained in this SOW and AIE Next P-Spec. The test program shall include planning, execution and assessment of system performance against the requirements. Testing objectives include determination and execution of corrective actions and subsequent demonstrations necessary for the System to meet requirements; performance of tests to support additional capabilities as necessary; support of maintenance testing; and validation of system level training. The Contractor's testing methodologies shall address how future system enhancements will be tested and validated. The Contractor shall perform the tests described in the following sections. The Contractor shall provide personnel, equipment, instrumentation and supplies necessary to perform or support all testing activities, unless otherwise indicated. Testing procedures need to be developed with Program input not just written by the contractor.

3.2.6.7.1 Test Readiness Review (TRR). Prior to any test, the Government will conduct a TRR at each Installation. The Contractor shall provide to the Government an integrated System Installation and Checkout Test Report IAW CDRL A020 and a letter of test readiness that the installed System is ready for testing. The Contractor shall attend test readiness review meetings, prepare minutes, provide required documentation and assist in the resolution of issues or concerns. Discrepancies in the documentation, design or training shall be corrected prior to the conduct of all test events and may involve re-test and re-training of personnel at Contractor's expense.

3.2.6.7.2 Production Qualification Test (PQT): AIE System Laboratory Testing. The Contractor shall conduct PQT at the Laboratory. The Contractor shall prepare a Test Plan IAW CDRL A021 and Test Procedures IAW CDRL A022 to verify all requirements defined in the AIE Next P-Spec. The integrated System will be tested to verify system performance. The Contractor shall provide a Test Inspection Report IAW CDRL A023. At the conclusion of testing and upon Government acceptance, the hardware, software, and network equipment will become the property of the Government.

3.2.6.7.3 Performance Verification Test (PVT): Government Acceptance Testing. The Contractor shall conduct PVT at each operational location immediately upon completion of installation. The Contractor shall prepare a Test Plan IAW CDRL A021 and Test Procedures IAW CDRL A022 to verify all requirements defined in the AIE Next P-Spec. The integrated System will be tested to verify system performance. The Contractor shall provide a Test Inspection Report IAW CDRL A023. At the conclusion of testing and upon Government

acceptance, the hardware, software, and network equipment will become the property of the Government.

The objective of PVT is to ensure the requirements in AIE Next P-Spec have been met at the operational site and the system meets its time-related performance requirements as verified. The objective, as described in CDRL A021, is to ensure that the System meets: an Ao of 97% and system reliability measured as a MTBF of 1440 hours at a minimum confidence level of 80%. For the purpose of collecting Reliability, Availability and Maintainability (RAM) data, the System shall be defined as one ACP with two lanes. For Installations with multiple ACPs and any ACP with more than two lanes, the data shall be normalized to the System. The Contractor shall conduct verification by capturing RAM data for one year at the first installed operational site to determine system compliance with RAM requirements.

3.2.6.7.4 Test Failures. The Government may terminate testing at any time the System fails to perform as specified in the Contract. Upon termination of testing, the Contractor shall commence an assessment of all failures, cause of failures, and prepare a Failure Analysis and Corrective Action Report (FACAR) IAW CDRL A024 and SOW section 3.2.6.7.5. The Contractor shall correct all failures and summarize IAW CDRL A023. The Contractor shall perform a retest IAW CDRL A021.

3.2.6.7.5 Failure Analysis and Corrective Action Report (FACAR). In the event of system/test event failure, the Contractor shall conduct an analysis of the failure and prepare a FACAR IAW CDRL A024. The Contractor shall track all failures to include Help Desk trouble tickets, identify failure trends, and propose corrective action to the Government for approval. The Contractor shall obtain Government approval prior to closing any FACAR. The Contractor shall maintain a library of identified issues and resolution until the end of the contract. Status of system failures shall be included in the Contractor's Progress, Status & Management Report.

3.2.6.8 Configuration Control Board (CCB). The Government is the CM decision authority and will manage/chair the AIE System CCB throughout the life of the contract. The Government will review/approve Class I (Emergency), Class II (Urgent) or Class III (Routine) designation for all changes. The Contractor shall participate in and support the CCB and conduct configuration control activities IAW PM-FPS CM Plan.

3.2.6.8.1 Configuration Management Plan. The Contractor shall develop and deliver a Configuration Management Plan IAW CDRL A025. The Contractor shall comply with the PM-FPS CM procedures for all equipment, hardware and system software. The Contractor shall provide configuration item identification and control activities of all System hardware and software as part of the AIE CM process. All changes will be approved by the CCB IAW the PM-FPS CM Plan.

3.2.7 Logistics Planning

The contractor shall implement an Integrated Logistics Support (ILS) program to ensure that supportability design criteria and characteristics are considered and incorporated into the design that meet the operational availability requirements of AIE Next Performance Specifications.

3.2.7.1 Total Package Fielding (TPF). The Contractor shall utilize TPF concepts IAW AR 700-142.

3.2.7.1.1 Contractor Logistics Support (CLS). The Contractor shall provide 12 months of CLS and support for transition to Government sustainment for all AIE system deployments, technology insertions, and technology refreshes executed under the AIE Next contract. CLS shall include all warranty (to include IA); software license renewals IAW CDRL A039; service agreements; 24/7 Help Desk and repair; scheduled and unscheduled field level maintenance above basic operator maintenance task and supply support, less consumables (such as printer supplies and identification card stock). The Contractor shall integrate and field a sustainable capability that provides minimal maintenance, logistics support, reduced manpower and personnel requirements, effective sustainable training, necessary design interface, technical data, computer resource support, adequate packaging, handling, storage and transportation capabilities. Any additional cost beyond the pre-negotiated CLIN price for labor, travel, and materials shall not be charged to the Government. This includes any associated cost with the repair/replacement of AIE system/component failures that are not the result of Government / User error.

3.2.7.1.2 Sustainment Transition Plan. The Contractor shall deliver a Sustainment Transition Plan IAW CDRL A026 for transitioning from CLS to centralized sustainment for each Installation. CLS warranty shall remain in effect until 90 days after the final Transition Plan is submitted to the Government regardless of the 12-month CLS POP.

3.2.7.1.3 Integrated Logistics Support Plan (ILSP). The Contractor shall deliver an Integrated Logistics Support Plan (ILSP) IAW CDRL A027. The ILSP shall include processes, procedures, metrics and documentation to be used during performance of CLS. As part of the first DO, the Contractor shall perform a Logistics Demonstration (LD) at the System Laboratory. The demonstration shall be conducted upon successful completion of PQT. The LD shall be tailored to document/verify the ILSP.

3.2.7.1.4 Level of Repair Analysis (LORA). The Contractor shall conduct a LORA IAW CDRL A028. The Contractor shall define the actions and support necessary to ensure that the system maintains Operational Readiness IAW AIE Next P-Spec.

3.2.7.1.5 Maintenance Management. The Contractor shall develop and deliver a Maintenance Support Plan IAW CDRL A029, Maintenance Service Report IAW CDRL A030, Logistics Management Information Summaries IAW CDRL A031 and Logistics Management Information Data Products IAW CDRL A032. The Contractor shall identify required resources to implement maintenance concepts and requirements. When formulating the maintenance concept, analysis of the proposed work environment on the health and safety of maintenance personnel shall be considered.

3.2.7.1.6 Manpower and Personnel. The Contractor shall identify personnel resources and skill sets required to operate and support equipment throughout the life of the System. CLS Manpower requirements shall be based on related CLS elements and predicated on accomplishing the logistics support mission.

3.2.7.1.7 Item Unique Identification (IUID) Plan. The Contractor shall identify required repair parts, spares and all supplies. The Contractor shall develop an IUID Plan IAW CDRL

A033 for all parts requiring IUID tags IAW Identification Marking of US Military Property MIL-STD-130N. The IUID tags shall be permanently affixed to the parts prior to delivery to the Government.

3.2.7.1.8 Diminishing Manufacturing Sources and Material Shortages (DMSMS) Plan. The Contractor shall minimize materiel readiness risks by applying the DMSMS management and implementation plans, based on standardization directory (SD) - 22 DMSMS Guidebook. The Contractor shall provide a DMSMS Management Plan IAW CDRL A034. The Contractor shall notify the Government, via an Obsolescence Alert Notice, within 10 days of learning of components that have become obsolete on deliverable or diminishing manufacturing sources IAW CDRL A033. Configuration changes as a result of obsolescence shall be managed IAW the CM Plan.

3.2.7.1.9 Support Equipment. The Contractor shall identify equipment required to sustain the operation and maintenance of the System to ensure the Operational Readiness metrics are met IAW the AIE Next P-Spec. A list identifying the required support equipment for all systems shall be included in the ILSP IAW CDRL A027.

3.2.7.1.10 Help Desk. The Contractor shall support the Government centralized Help Desk that operates 24 hours / seven (7) days per week, during the 12-month CLS period, by providing trouble tickets/status updates for all issues related to AIE systems fielded by the contractor. The Contractor shall provide response to Help Desk submissions within 24 hours and commence repairs within 48 hours IAW CDRL A035. The Contractor's Help Desk solution shall be incorporated with the Government Help Desk, to include updated ticket status, providing the Government full visibility to all Help Desk data.

CLS help desk data will be organized and maintained by the contractor in near-real time via a database repository such as, but not limited to, 4Sight or JIRA such that it can be queried and exported for analysis. The Contractor shall provide the Government access to their database repository. The Contractor shall deliver a CLS Help Desk Ticket Report IAW CDRL A035. AIE help desk trouble ticket data will be imported and analyzed by a Reliability, Availability, and Maintainability (RAM) tool, an interface with dynamic data analytic capability.

Help Desk Trouble Ticket data fields will include at a minimum:

- Ticket Status: Open, Closed, Pending
- Installation: AIE Site
- Location: Location at Site, lane, ACP, NEC etc
- Failure Item: HW, SW, Training (user error), Support, Other
- Product Name: Item nomenclature and model/part number
- Description of Issue:
- Status: degraded (PMC) or down (NMC)
- Priority: high, medium, low
- Date Reported:
- Date FSR Assigned:
- Time on Ticket:
- Date FSR Resolved:
- Description of Troubleshooting:
- Description of Resolution:
- Part Removed (Name):

- Part Removed (Serial Number):
- Replacement Part Name: may be different due to obsolescence
- Replacement Part Serial Number:
- Root Cause: to include corrective action
- POC:
- POC Email:

3.2.7.1.11 Technical Data and Software Rights. The Contractor shall provide the rights in non-commercial technical data and software deliverables governed by the terms and conditions of this contract. Because the Government's rights in commercial software are governed by the licensor's commercial software license agreements (unless the license terms are inconsistent with Federal procurement law or do not otherwise satisfy user needs), the Offeror's proposal shall include all applicable commercial software license agreements related to commercial software deliverables.

3.2.7.1.12 Packaging, Handling, Storage and Transportation (PHS&T). The Contractor shall identify resources and processes required for materiel packaging/preservation, handling, storage and transportation to maximize availability and usability of the materiel IAW CDRL A027. The Contractor shall perform PHS&T processes during DO execution.

3.2.7.1.13 Repair Return Merchandise Authorization (RMA). IAW CDRL A040, the Contractor shall provide all necessary material, personnel, and associated resources to support non-warranty repairs to include replacement of damaged equipment and spares such as broken/malfunctioning handhelds, monitors, and other various pieces of onsite equipment.

3.2.7.2 Training. The Contractor shall identify, plan and implement an integrated strategy to train personnel to effectively operate and maintain the System throughout the life cycle. Training and training resources shall encompass the processes, procedures, techniques, equipment and materials used to train personnel to operate and support the System in the following roles: (a) System Administrator, (b) Registrar, (c) Operator (d) Maintainer and (e) Depot Level (Software and Hardware). The Contractor shall capture their integrated strategy in a Training Program Development and Management Plan IAW CDRL A037.

Specific training dates will be identified in associated Delivery Orders. Student to trainer ratio for Administrator, Registrar and Maintenance Training shall be five to one. Student to trainer ratio for Operator and Depot level courses shall be 10 students per one trainer. The Contractor shall provide Quick Reference Guides (QRGs) and a sustainment training package IAW Training Conduct Support Document Package CDRL A038. Except for Depot Level Training, all training will occur at each site following Government acceptance of system installation.

3.2.7.2.1 Depot Level Training (DLT). Depot level training will occur at the Government Laboratory with more emphasis placed on a hands-on approach than a classroom setting. Access to Lab equipment and facilities will be available for Depot Level training. Depot Level training shall entail two weeks of instruction minimum and focused on AIE hardware, software and cloud functionality to include wiring and configuration of all subsystems, configurations and system functions. Contractor shall provide DLT course package for Government review 60 days prior to training start dates IAW CDRL A038. Training package includes relevant course materials, OJT hands on instruction.

3.2.7.3 Inventory Management. The Contractor shall perform associated logistical support and inventory management functions to maintain and track equipment and software accountable (unless provided as Government furnished equipment) under the contract. This task includes acquiring and managing all parts and materials necessary to support the actions required as specified in delivery orders. Logistics support and inventory management includes but is not limited to, the equipment, spares, and licensing inventory management, shipping and receiving, ordering, tracking, shipping, expediting purchases, warehousing, storage, and staging. The Contractor shall provide a summary of Supply Chain Management (SCM) functions (i.e. procurement, inventory, order/ship times, on hand balances, etc.) in the CDRL A017 monthly report.

3.2.7.4 Supply Chain Risk Management (SCRM). Contractor shall develop, maintain, and periodically update SCRM plans at no cost to the Government. SCRM plans are intended to reduce performance and security risks of the products sold, installed, and maintained throughout the life-cycle. SCRM plans shall include sufficient detail for the Government to determine that the Contractor reasonably understands its supply chain and the associated risks. The Contractor shall manage the risk to ensure counterfeit or illegally modified products are not shipped.

3.2.8 Sustainment Option

The Contractor shall provide sustainment support for all installations operating the AIE system for base access control. This includes 98 installations fielded under the previous AIE-3 production and deployment contract as well as all installations fielded under this contract. This sustainment scope does not include the 12-month CLS period. The Contractor shall assign a Sustainment Project Lead to direct, prioritize, schedule, and control all AIE sustainment related activities. Under this Sustainment Option, the Contractor shall:

- Monitor all deployed AIE systems
- Execute monthly IAVA updates
- Maintain Windows Server Update Service (WSUS) expertise; track, download, and install Cybersecurity Vulnerability Alerts (IAVAs)
- Perform Assured Compliance Assessment Solution (ACAS) Nessus scanning
- Support certification and accreditation documentation preparation
- Ensure timely synchronization of Help Desk data to the ARAM tool.
- Manage Software license procurement
- Prepare Assess and Authorize (A&A) packets for Authority To Connect (ATC) packages
- Prepare POA&M original and update packets in EMASS, coordinate ACA events, staff packets and documents through ACAs to attain and retain Approval to Operate (ATO)
- Maintain system accreditation through yearly Federal Information Security Management Act (FISMA) assessments
- Support and complete Command Cyber Readiness Inspections (CCRI), should they occur
- Conduct AIE regression testing for IAVA and full releases
- Investigate, debug, and troubleshoot help desk tickets
- Develop testing protocol for various aspects, such as usability, database impact, error and bug finding, regression testing, and implementation scenarios.
- Identify, analyze and create detailed records of problems that appear during testing, such as software defects, bugs, functionality issues, and output errors, and work

directly with software developers to find solutions and develop retesting procedures.

- Track problems, resolutions, and bug fixes throughout testing and create a comprehensive database of defects and successful mitigation techniques.
- Create detailed, step-by-step documentation of test procedures for each release as needed
- Design and implement automated testing tools when possible, and update tools as needed to ensure currency and accuracy
- Troubleshoot database anomalies, problems, inefficiencies and data loss
- Compile and present monthly progress and operational reports to the management team
- Manage technical support queries on major and minor bug fixes and other issues
- Integrate updates and new features to existing software and hardware
- Perform routine checks to ensure hardware and systems are stable and operating efficiently
- Develop protocols for checking for and repairing software bugs
- Navigate workload ticketing system and resolve tickets in order of urgency
- Answer technical queries and assist users
- Assist with obsolescence management, inform the PM of obsolescence challenges
- Perform STIG implementation
- Ensure that the network infrastructure is up and running
- Configure, add, and delete file system
- Provide system analysis, troubleshooting and integration support for HBSS (Host-Based Security Solution).
- Install, troubleshoot, and sustain the McAfee HBSS ePO agent, handlers, Super-Agent Distributed Repository (SADR) servers for a Hybrid DISA Milcloud enclave.
- Deploy and manage client End Point Products, collect, secure and manage activities.
- Support daily operations and deployment of all HBSS modules on server and workstation nodes, review threat events in Host Intrusion Prevention System (HIPS), analyze firewall rule sets and maintain HIPS trusted network policy for network devices, applications and services.
- Apply applicable STIGS, IAVM directives and CTO instructions to the architecture.
- Monitor and maintain network event logs
- Maintenance, implementation, and support of Splunk (Indexers, Forwarders, Search - Heads Setup etc).
- Maintain virtualization technologies (VMware, etc).
- Monitor Apps/Dashboards for license usage and Application errors.
- Maintain Linux and Windows agents for Splunk administration with a solid understanding of the Splunk system.
- Create/update operational documentation for maintaining the Splunk infrastructure.
- Set up Splunk Forwarding for new application tiers introduced into the environment.
- Identify bad searches/dashboards and partnering with the creators to improve performance.
- Troubleshooting Splunk performance issues / Opening support cases with Splunk.
- Monitor the Splunk infrastructure for capacity planning and optimization.

3.2.9 Security

3.2.9.1 Clearances. The Contractor shall provide personnel with appropriate clearance levels to fulfill requirements set forth in each DO without impact to cost, schedule, or quality. Most of the Contract will be Controlled Unclassified Information (CUI). All Contractor personnel shall be required to access, view, possess, process and/or use information designated as CUI. Contractors who require access to NEC and DOIM facilities must have a SECRET clearance. Individual requirements for SECRET-eligible personnel shall be established at the DO level. DOs requiring such access will be awarded IAW a revised DD Form 254 detailing appropriate access and outlining the specific security requirements. The Contracting Officer or Contracting Officer's Representative (COR) shall apprise the Contractor of any increased security requirements. The Contractor shall submit completed clearance packages within ten calendar days of identification of any increased security requirements.

3.2.9.2 DoD Common Access Cards (CAC). Contractor personnel requiring recurring access to DoD Installations may (at the discretion of the Government) be issued DoD CACs. The Contractor shall furnish all requested information required to facilitate the use and possession of the CACs and/or badges. The Contractor's Program Manager shall be responsible for ensuring that all identification badges issued to Contractor employees are returned immediately following the completion of the Contract, relocation or termination of an employee and/or upon request of the Contracting Officer or the COR.

3.2.9.3 Cybersecurity / Information Technology (IT) Training. All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

3.2.9.4 Anti-Terrorism (AT) Training. All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled-access areas shall complete AT Level I awareness training within 15 calendar days after the 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 within 15 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: http://jko.jten.mil

3.2.9.5 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 Anti-Terrorism Officer (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 15 calendar days of contract award and within 15 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

3.2.9.6 Army Training Certification Tracking System (ATCTS) Registration. All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services and must

successfully complete the DOD Cybersecurity Awareness prior to access to the IS and then annually thereafter.

3.2.9.7 Operations Security (OPSEC) Plan. The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1.

3.2.9.8 OPSEC Training. Per AR 530-1 Operations Security, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter.

3.2.9.9 Threat Awareness Reporting Program. For all contractors with security clearances. 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 AR 381-12, section 2-4b.

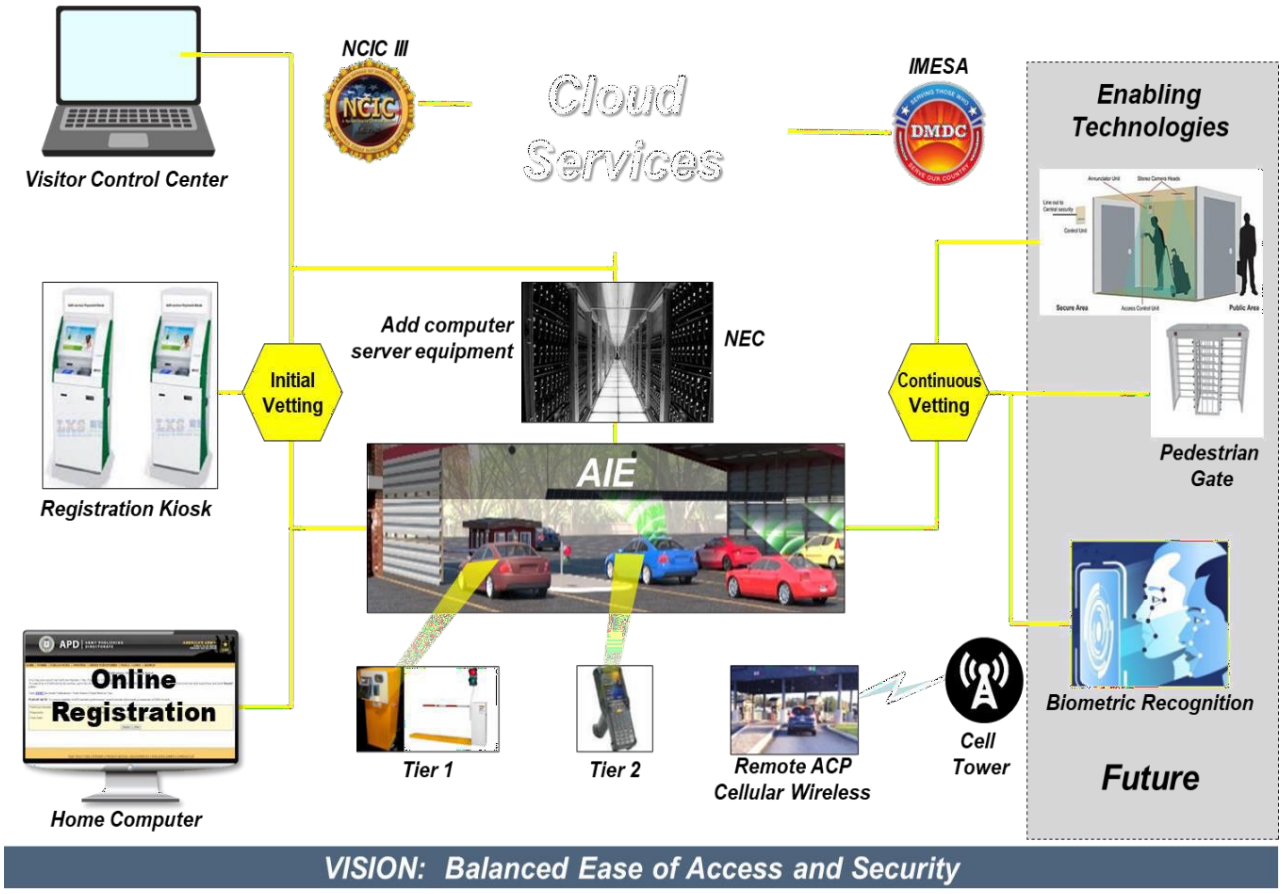
3.2.9.10 Access and General Protection/Security Policy and Procedures. Contractor and all associated sub-contractors employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by 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.

3.2.10 Health and Safety

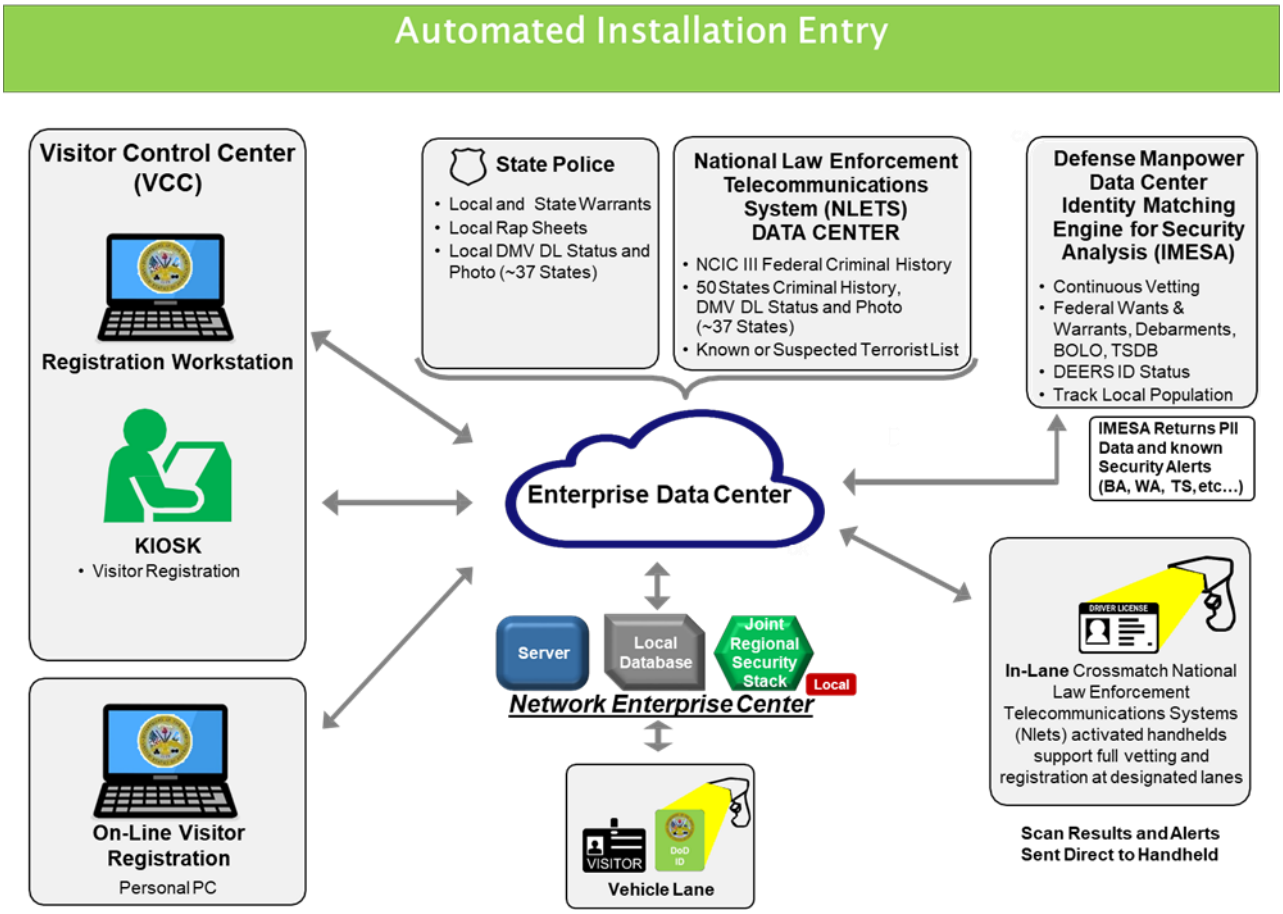
The Contractor shall update and maintain the programmatic environmental compliance, health and safety program compliance and 29 Code of Federal Regulations (CFR) 1926 Occupational Safety and Health Administration (OSHA) compliance. The Contractor shall develop a Safety Assessment Report IAW CDRL A036.

APPENDIX A:

Operational View (OV-1) and System View (SV-1)



OV-1


Automated Installation Entry
Visitor Control Center (VCC)
Registration Workstation
KIOSK
• Visitor Registration
On-Line Visitor Registration
Personal PC
State Police
• Local and State Warrants
• Local Rap Sheets
• Local DMV DL Status and Photo (~37 States)
National Law Enforcement Telecommunications System (NLETS) DATA CENTER
• NCIC III Federal Criminal History
• 50 States Criminal History, DMV DL Status and Photo (~37 States)
• Known or Suspected Terrorist List
Defense Manpower Data Center Identity Matching Engine for Security Analysis (IMESA)
• Continuous Vetting
• Federal Wants & Warrants, Debarments, BOLO, TSDB
• DEERS ID Status
• Track Local Population
IMESA Returns PII Data and known Security Alerts (BA, WA, TS, etc…)
Enterprise Data Center
Server
Local Database
Joint Regional Security Stack
Local
Network Enterprise Center
VISITOR
DoD ID
Vehicle Lane
In-Lane Crossmatch National Law Enforcement Telecommunications Systems (Nlets) activated handhelds support full vetting and registration at designated lanes
Scan Results and Alerts Sent Direct to Handheld

SV-1